

Welcome

Dear Microsoft Employee:

Welcome to Microsoft. As an employee here, you have the opportunity to share in the excitement of shaping the future success of our company. We know you will find your work here challenging and rewarding, and we believe your contribution will be meaningful - one that will give you real satisfaction.

Microsoft has a strong tradition of excellence and innovation. We recognize that our employees have created that tradition and are largely responsible for our success. As a result, we have a strong commitment to providing the finest possible work environment and many opportunities for personal satisfaction and growth.

This handbook provides you with valuable information about our history, policies, and benefits. Please take the time to review this handbook carefully, and discuss any questions or suggestions you may have with your manager or your Human Resources representative.

Sincerely,

Bill Gates

INDEX

I. Microsoft Introduction	7
II. Microsoft China	7
III. Microsoft Standards of Business Conduct	9
Great People with Great Values	9
Microsoft Values	10
Why Microsoft Has Standards of Business Conduct.....	10
How to Use the Standards of Business Conduct	10
Compliance with the Standards of Business Conduct	11
Microsoft's Standards of Business Conduct.....	12
Microsoft's Business Conduct and Compliance Program	16
IV. Microsoft Office Guidelines	19
General Company Guidelines	19
Disciplinary Rules on Violations of Company Policies & Labor Discipline	20
Information Technology Guidelines and Policy	33
Confidential/Proprietary Information or Trade Secret.....	36
How Should Employee Protect Microsoft's Property – Intellectual Property	38
Open Source Software	40
Proper Use of Microsoft and Third Party Copyrighted Materials	42
Anti-Piracy Policy.....	43
Anti-Harassment and Anti-Discrimination.....	44
Company Access and Monitoring Information and Property	45
Conflict of Interest.....	46
Rules for the Use of E-mail and the Internet	49
Employee's Personal Information Processing Policy of Microsoft China	50
V. Microsoft China Human Resources Information	65
Compensation Philosophy	665
Payroll Information	665
Stock Award and Employee Stock Purchase Plan	69
Social Benefits and Employee Benefits	70
MS Vacation User Guidance	81
How to submit leave supporting document(s).....	83
How to submit Voluntary Termination Request	84
Manage Your Personal Data	84
Performance and Development.....	887
Inbound / Work Permit / Residence Permit Assistance for Foreign Passport Holders*	88
Other Information.....	88
VI. MICROSOFT CHINA EMPLOYEE BUSINESS TRAVEL POLICY and GUIDELINE	89
Explore MSTravel.....	89
Company Travel Policy & Guidance	89
China Available information	90
VII. MICROSOFT CHINA EMPLOYEE BUSINESS EXPENSES REIMBURSEMENT	93
Meal and Entertainment	93
Employee Personal Vacation	93
Telephone Charges	94
Travel Insurance	94
Miscellaneous.....	95
Reimbursement Procedure.....	95
Notes of Reimbursement	96
VIII. MICROSOFT REAL ESTATE & FACILITIES SERVICES.....	101
Main Reception.....	101

Employee Meal Service.....	101
Office Equipment.....	102
Stationery Service and Business card	102
Mail Service	102
Office Space Management	103
In-Office Move Service	103
Pantry Services	103
Incident Reporting	104
Facility Management Service Information	104
RE&F Global Facilities Service Center Hotline.....	104
IX. Microsoft Digital (formerly Microsoft IT) HANDBOOK	105
Microsoft Digital Service	105
System Initial Settings).....	105
About Microsoft Network Environment.....	115
Microsoft Information Services General Use Standard	116
Related Web Sites and Software Installation	116
X. MICROSOFT GLOBAL SECURITY INSTRUCTION	117
Access Control	117
Visitor Management Procedure	118
Theft Prevention.....	118
Personal Safety	120
Emergency Preparedness.....	120
Travel Safety	121
Social Engineering.....	122
Global Security Contacts.....	123
XI. Others.....	125
Useful Website Links.....	125
Attachment --- Receipt signed by the Microsoft China employee acknowledging that he/she has read the Employee Handbook	127

Reading instructions:

This handbook is provided for full time employees (FTE) of Microsoft (China) Co., Ltd. ("Microsoft" or "company"). Microsoft's continuing growth and advancement require that its benefits and policy systems change in line with this. Microsoft has the right to make the corresponding revisions to this Employee Handbook from time to time in accordance with changes in Chinese laws or changes in Company benefits, policies or Company rules governing internal production and management. Microsoft will, by announcement on the intranet or by e-mail, notify its employees of the relevant changes, explain the details of such relevant changes and state the effective date of the new policy. The employee acknowledges and agrees that he/she is also obligated at all times to check the various relevant web sites of the Company to understand its latest policy and rules for observation.

Any questions and/or recommendations related to the changes shall be directed to Human Resources Department within 15 calendar days after receiving Company's notice.

Remark: At the execution of your Employment Contract, please send back the attachment with your signature to HR for the purpose of archive..

Any questions, please visit HRWeb and submit your question via ASK HR

<https://microsoft.sharepoint.com/sites/hrw/AskHR/Pages/AskHR.aspx?appTenant=HRweb&srcURL=http://hrweb/Pages/default.aspx>)

I. MICROSOFT INTRODUCTION

Microsoft Company Mission

In the era of an intelligent cloud and an intelligent edge, Microsoft's mission is to empower every person and every organization on the planet to achieve more.

Microsoft Corporate Values

Our values align to our mission to empower every person and organization on the planet to achieve more. They support our culture and serve as a declaration of how we treat each other, our customers and our partners.

- **Respect:** We recognize that the thoughts, feelings, and backgrounds of others are as important as our own.
- **Integrity:** We are honest, ethical, and trustworthy.
- **Accountability:** We take full responsibility for our decisions, actions, and results.

Microsoft (NASDAQ: MSFT) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more. **For more information about Microsoft**, please refer to the official website <https://news.microsoft.com/facts-about-microsoft/#BusinessOrganization> and intranet <https://microsoft.sharepoint.com/>

II. MICROSOFT CHINA

Started from its establishment in 1975, Microsoft has become a leading software, service, devices and solution provider around the world. Since the establishment of its first China office in Beijing in 1992, Microsoft has rapidly expanded its business across the country under its strategy of long-term investment and development. Microsoft has been working closely with customers and industry partners to realize innovation and both localize and land Microsoft technologies and solutions in China. Microsoft boasts a robust partner ecosystem with 17,000 partners, which create a powerful partner ecosystem. With a roster that includes Microsoft Azure, Windows, Office, Dynamics, SQL Server, LinkedIn, Bing, Surface and Xbox, our products and services are built for a broad ecosystem of developers, partners, customers and consumers. In a new era of intelligent cloud and intelligent edge, Microsoft is offering Chinese consumer, enterprise and institutional users the experiences that could enhance productivity to its fullest potential by leveraging cloud computing, big data, artificial intelligence, devices and hardware that are secure and reliable.

For more information, please visit:

<https://www.microsoft.com/zh-cn/>
[GCR Staff Bulletin Group](#)

Microsoft Asia-Pacific Research and Development Group

Microsoft Asia-Pacific Research and Development Group (ARD) is a complete innovation chain of fundamental research, technology incubation, product development, and strategic

partnerships. It is the largest and most comprehensive R&D base for Microsoft outside of the United States. At ARD, over 3000 scientists and engineers work at the cutting-edge of technology, innovating solutions that impact millions of people around the world on a daily basis. With campuses in Beijing, Shanghai, Shenzhen, and Suzhou, our engineers and researchers span Microsoft's major engineering divisions and product lines, including Microsoft Azure, Microsoft 365, Microsoft Dynamics 365, Bing, Ads, Visual Studio, Surface, HoloLens, Xbox, Microsoft Translator, Microsoft Cognitive Services, , etc.

ARD supports Microsoft's global mission for worldwide research, technological innovation, and product development, further strengthening cooperation and exchanges with industry colleagues and academic institutions in the region.

The Asia-Pacific region plays a key role in Microsoft's global strategy, and by cultivating nascent local talent, ARD delivers highly localized R&D for emerging markets and innovations in products, services and tools for the globe, while actively cultivate a cooperative, innovative, mutually beneficial industrial ecosystem.

.

Please visit <https://www.microsoft.com/zh-cn/ard>

III. MICROSOFT STANDARDS OF BUSINESS CONDUCT

Great People with Great Values

Dear Fellow Employee:

Microsoft aspires to be a great company, and our success depends on you. It depends on people who innovate and are committed to growing our business responsibly, people who dedicate themselves to really satisfying customers, helping partners, and improving the communities in which we do business, people who are accountable for achieving big, bold goals with unwavering integrity, people who are leaders, who appreciate that to be truly great, we must continually strive to do better ourselves and help others improve.

We must expect the best from ourselves because who we are as a company and as individuals is as important as our ability to deliver the best products and services. How we manage our business internally and how we think about and work with customers, partners, governments, vendors and communities - impacts our productivity and success. It's not enough to just do the right things; we have to do them in the right way.

The Standards of Business Conduct are an extension of Microsoft's values and the foundation for our business tenets. They reflect our collective commitment to ethical business practices and regulatory compliance, and they provide information about Microsoft's Business Conduct and Compliance Program. At a high level, they summarize, and are supported by, the principles and policies that govern our global businesses in several important areas: legal and regulatory compliance; trust and respect of consumers, partners and shareholders; asset protection and stewardship; creation of a cooperative and productive work environment; and commitment to the global community.

These Standards of Business Conduct provide information, education and resources to help you make good, informed business decisions and to act on them with integrity. In addition, managers should use this resource to foster, manage and reward a culture of accountability and integrity within their groups. Working together, we can continuously enhance our culture in ways that benefit customers and partners, and that strengthen our interactions with one another. Then we can truly achieve our mission of enabling people and businesses throughout the world to realize their full potential.

All Microsoft employees are responsible for understanding and complying with the Standards of Business Conduct, applicable government regulations and Microsoft's policies. As Microsoft employees, you also have a responsibility to raise compliance and ethics concerns through our established channels. This is the way to ensure that Microsoft is and continues to be a great company of great people.

Satya Nadella
CEO

Microsoft Values

- Integrity and honesty
- Passion for customers, partners, and technology
- Open and respectful with others and dedicated to making them better
- Willingness to take on big challenges and see them through
- Self-critical, questioning, and committed to personal excellence and self-improvement
- Accountable for commitments, results, and quality to customers, shareholders, partners, and employees

Why Microsoft Has Standards of Business Conduct

As responsible business leaders, it is not enough to intend to do things right, we must also do them in the right way. That means making business decisions and taking appropriate actions that are ethical and in compliance with applicable legal requirements. As we make these decisions, Microsoft's values must shine through in all our interactions. The Standards of Business Conduct are an extension of Microsoft's values and reflect our continued commitment to ethical business practices and regulatory compliance.

By following the guidance provided in this publication, we are acknowledging our individual and collective responsibilities to manage our business activities with integrity as we pursue our mission of enabling people and businesses throughout the world to realize their full potential.

How to Use the Standards of Business Conduct

Microsoft's Standards of Business Conduct summarize the regulatory requirements and business practices that guide our decision making and business activities. The Standards contain basic information about our policies as well as information about how to obtain guidance regarding a particular business practice or compliance concern. It is essential that you thoroughly review this publication and make a commitment to uphold its requirements.

The Standards of Business Conduct are not intended to cover every issue or situation you may face as a Microsoft employee. Nor does it replace other more detailed policies or guidelines. You should use the Standards as a reference guide in addition to Microsoft's policies and guidelines, including the Employee Handbook, required for your specific job. For example, the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Corporate Controller and other employees of the finance organization must also comply with the Microsoft Finance Code of Professional Conduct. Microsoft reserves the right in its sole discretion to modify or eliminate any of the Standards' contents without prior notice. Individual business units may also adopt standards of professional conduct for their areas. It is your responsibility to be fully aware of these Standards and follow them.

If you need details on a specific policy, you may refer to the online version of the Standards of Business Conduct at <http://businessconduct>

If you need guidance regarding a business practice or compliance issue or wish to report a possible violation, talk to your direct managersupervisor, another member of management team, your Human Resources Generalist, or your Corporate, External, & Legal Affairs (CELA) contact. You may also call the Business Conduct Line at 1-877-320-MSFT (6738). If you are calling from outside the United States, you may make a collect call to the Business Conduct Line by accessing

an international operator and asking to place a collect call to 1-704-540-0139. The Business Conduct Line is a dedicated, toll-free phone line that is available to you 24 hours a day, 7 days a week, and 365 days a year. It is operated by an external third-party vendor that has trained professionals to take your calls, in confidence, and report your concerns to the Microsoft Director of Compliance for appropriate action. Your phone calls to the Business Conduct Line may be made anonymously.

If you are a Microsoft employee or vendor with access to our corporate intranet and wish to send a confidential e-mail to the Director of Compliance, you may do so by e-mailing the Business Conduct and Compliance alias (buscond@microsoft.com). A confidential e-mail may be delivered via the Internet by e-mailing msft.buscond@alertline.com. These e-mails will be received by a third-party vendor, who will remove your contact information prior to forwarding a summary of the e-mail to the Office of Legal Compliance.

You may also send a letter to the Director of Compliance at Microsoft Corporation, CELA, One Microsoft Way, Redmond, WA 98052 or send a confidential fax to 1-425-705-2985. Letters and faxes sent to the Director of Compliance may be submitted anonymously if you choose to do so.

If you have a concern regarding a questionable accounting or auditing matter and wish to submit the concern confidentially or anonymously, you may do so by sending an e-mail to msft.buscond@alertline.com, calling the Business Conduct Line, or sending a letter or fax to the Director of Compliance as outlined above.

Microsoft will handle all inquiries discreetly and make every effort to maintain, within the limits allowed by the law, the confidentiality of anyone requesting guidance or reporting a possible violation.

Compliance with the Standards of Business Conduct

The Microsoft Standards of Business Conduct are a general guide to the company's standards of business practices and regulatory compliance. Its requirements apply to Microsoft Corporation, to all subsidiaries, or affiliates in which Microsoft Corporation directly or indirectly owns more than 50 percent of the voting control ("Controlled Affiliates"), and to all directors, officers, and employees of each. All references to "Microsoft" include Microsoft Corporation and all Controlled Affiliates unless otherwise specified. All references to "employees" include directors, officers, and employees of Microsoft Corporation and its subsidiaries or affiliates.

Failure to read and/or acknowledge the Standards of Business Conduct does not exempt an employee from his/her responsibility to comply with the Standards of Business Conduct, applicable laws, regulations, and Microsoft policies that are related to his/her job.

Microsoft is a global company, and our business operations are subject to the laws of many different countries. Microsoft employees doing business internationally must comply with applicable laws and regulations and uphold the Standards of Business Conduct at all times. Cultural differences or local laws and customs may require a different interpretation of our Standards. If this situation arises, always consult your manager, CELA manager, or the Director of Compliance before taking any action.

The Standards are not intended to and do not create an employment contract, and do not create any contractual rights between Microsoft and its employees or create any express or implied promise for specific treatment in specific situations. Your employment relationship with Microsoft

can be terminated at any time for any reason with or without cause unless otherwise required by local laws outside the United States or a written contract signed by a vice president.

Our Commitment: Integrity in All Our Interactions

Each day we interact with a variety of individuals and groups—including our customers, partners, competitors, co-workers, shareholders, vendors, government and regulatory agencies, and the communities in which we operate. We are committed to interacting with all of these audiences in a respectful, ethical manner and in compliance with applicable laws and regulatory requirements.

Microsoft's Standards of Business Conduct

We manage our business in compliance with applicable laws and regulatory requirements.

Regulatory Compliance: We are aware of and obey the laws and regulations that govern the global management of our business. We are responsible for understanding these laws and regulations as they apply to our jobs and for preventing, detecting, and reporting instances of non-compliance to a member of Microsoft management, Human Resources, CELA, the Director of Compliance, or the Business Conduct Line. We don't tolerate any disrespectful behaviour of law and regulation.

Lobbying: We recognize our right and responsibility to lobby on behalf of issues that affect our company and business operations. We conduct our lobbying activities in compliance with applicable laws and regulations governing these activities.

Political Activities and Contributions: Microsoft employees are encouraged to exercise their right to participate in political activities. Any decision to become involved is entirely personal and voluntary. Employees' personal political activities are done on their own time and with their own resources. Without prior approval of CELA, we shall not indicate that we are acting or speaking on behalf of or for Microsoft.

Regulatory Investigations, Inspections, and Inquiries: We are direct, honest, and truthful in our discussions with regulatory agency representatives and government officials. During investigations, inspections, and inquiries we work with Microsoft's CELA members and cooperate by responding to appropriate requests for information.

International Business Activities: Microsoft acknowledges and respects the diverse cultures, customs, and business practices it encounters in the international marketplace. Microsoft will comply with both the applicable U.S. laws and regulations that govern its operations and local laws wherever it does business.

Sensitive Payments: Microsoft complies with the anti-corruption laws of the countries in which it does business, including the United States Foreign Corrupt Practices Act ("FCPA"). In compliance with the FCPA, Microsoft and its agents/partners/representatives will not make any direct or indirect payments or promises of payment to foreign government officials for the purpose of inducing the individual to misuse his/her position to obtain or retain Microsoft business.

Anti-Boycott Requirements: Microsoft complies with U.S. law that prohibits participation in

international boycotts that are not sanctioned by the U.S. government.

Export Control: In order to protect U.S. national security, implement U.S. foreign policy, and preserve scarce resources, the United States government restricts the export of certain technology and products, including certain computer software and technical goods and data. We observe restrictions applicable to our business placed on the export and re-export of a U.S. product or component of a product, good, service, or technical data.

Fair Competition and Antitrust: As a global business, we encounter laws and regulations designed to promote fair competition and encourage ethical and legal behavior among competitors. Antitrust laws and fair competition laws generally prohibit any activity that restrains free trade and limits competition. We conduct our business in compliance with these laws.

We build and maintain the trust and respect of our customers, consumers, partners, and shareholders.

Responsible Leadership: We manage our business responsibly in order to maintain the confidence, respect, and trust of our customers, consumers, partners, shareholders, and other audiences. We are committed to acting with integrity, investing in new product development, being responsive and accountable to our customers and partners, and remaining a leader in our field. We understand the responsibility that comes with being a worldwide technology and business leader and accept our unique role in both our industry and the global business community.

Product and Service Quality: Microsoft's products and solutions are developed and managed to meet the expectations of our customers, consumers, and partners for high quality and exceptional service. We continually seek new ways to improve our products, service, and responsiveness.

Communication: We establish and maintain clear, honest, and open communications; listen carefully; and build our relationships on trust, respect, and mutual understanding. We are accountable and responsive to the needs of our customers, consumers, and partners and take our commitments to them seriously. Our advertising, sales, and promotional literature seeks to be truthful, accurate, and free from false claims. Unless there is restriction from competition or law, we will provide our shareholders with appropriate information timely.

Obtaining Competitive Information: Microsoft has an obligation, and is entitled, to keep up with developments in our industry, including obtaining information about our competitors. We obtain information about our competitors through honest, ethical, and legal methods.

Fair Information Practices: Our business is built around technologies to manage information, and we treat that information with confidentiality and integrity. We are committed to creating a trustworthy environment for Internet users, and continually striving to protect their online privacy is at the core of this commitment. We have adopted privacy practices, developed technological solutions to empower individuals to help protect their online privacy, and continue to educate consumers about how they can use these tools to manage their personally identifiable information while they use the Internet.

Vendors: Microsoft vendors must adhere to the highest standards of ethical behavior and

regulatory compliance and operate in the best interest of Microsoft. Vendors are expected to provide high-quality services and products while maintaining flexibility and cost-effectiveness. All vendors are required to read and comply with the Microsoft Vendor Code of Conduct and, when appropriate, train their employees and representatives to ensure that they are aware of Microsoft's expectations regarding their behavior. We do not engage in any unethical or illegal conduct with our vendors. We do not accept incentives such as kickbacks or bribes in return for conducting business with them.

We are responsible stewards in the use, protection, and management of Microsoft's assets.

Financial Integrity: We honestly and accurately record and report business information. We comply with all local, state, and federal laws regarding record completion and accuracy. We require that financial transactions be executed in accordance with management's authorization, and recorded in a proper manner in order to maintain accountability for Microsoft's assets. Our financial information reflects only actual transactions and is in compliance with Microsoft and other applicable accounting practices.

Use and Protection of Assets: We wisely use and protect the assets of the company, including property (both physical and intellectual), supplies, consumables, and equipment. We use these assets exclusively for Microsoft's business purposes.

Fiscal Responsibility: Microsoft employees exercise good stewardship over and spend Microsoft's funds in a responsible manner.

Use of Information Technology: At all times, we should use good judgment and common sense; conduct ourselves ethically, lawfully, and professionally; and follow applicable authorization protocols while accessing and using company-provided information technology and its contents. In using these company assets and systems, we do not create, access, store, print, solicit, or send any material that is intimidating, harassing, threatening, abusive, sexually explicit, or otherwise offensive or inappropriate, nor do we send any false, derogatory, or malicious communications.

Intellectual Property: We comply with the laws and regulations that govern the rights to and protection of our own and others' copyrights, trademarks, patents, trade secrets, and other forms of intellectual property.

Creation, Retention, and Disposal of Records and Information Assets: We create, retain, and dispose of our business records and information assets, both written and electronic, as part of our normal course of business in compliance with Microsoft policies, and applicable regulatory and legal requirements.

Confidential and Proprietary Information: We respect our ethical and legal responsibilities to protect Microsoft's confidential/proprietary information or trade secret and proprietary non-public information and communicate it only as necessary to conduct Microsoft's business. We do not use this information for our personal advantage or for non-Microsoft business use, and maintain this confidentiality even after Microsoft no longer employs us.

Third-Party Software: We use software and other content information only in accordance with their associated licenses and/or terms of use. We prohibit the making or using of copies

of non-licensed copyrighted material, including software, documentation, graphics, photographs, clip art, animation, movie/video clips, sound, and music.

Insider Information and Securities Trading: In the course of doing business for Microsoft or in discussions with one of its customers, vendors, or partners, we may become aware of material non-public information about that organization. Information is considered "material" if there is a substantial likelihood that a reasonable investor would consider it important in making a decision to trade in the public securities of the company. Individuals who have access to this type of information are called "insiders." We discuss this information on a limited, "need to know" basis internally, and do not share it with anyone outside Microsoft. We do not buy or sell the public securities of a company, including our own, on the basis of such information, and we do not share ("tip") this information with others. Because of the extremely sensitive nature of and severe penalties associated with "insider trading" and "tipping," contact Microsoft's CELA before you buy or sell public securities in situations that could be of this nature.

Conflicts of Interest: Microsoft employees are expected to act in Microsoft's best interests and to exercise sound judgment unclouded by personal interests or divided loyalties. Both in the performance of our duties for Microsoft and our outside activities, we seek to avoid the appearance of, as well as an actual, conflict of interest.

Gifts and Entertainment: Microsoft policy and practice encourage the use of good judgment, discretion, and moderation when giving or accepting gifts or entertainment in business settings. Gift giving and entertainment practices may vary in different cultures; however, any gifts and entertainment given or received must be in compliance with law, must not violate the giver's and/or receiver's policies on the matter, and be consistent with local custom and practice. We do not solicit gifts, entertainment, or favors of any value from persons or firms with which Microsoft actually or potentially does business. Nor do we act in a manner that would place any vendor or customer in a position where he/she may feel obligated to make a gift, provide entertainment, or provide personal favors in order to do business or continue to do business with Microsoft.

Purchasing Decisions and Practices: In our purchasing decisions, negotiations, contract development, and contract administration we comply with the applicable laws and regulations that govern those relationships.

We promote a diverse, cooperative, and productive work environment.

Openness, Honesty, and Respect: In our relationships with each other, we strive to be open, honest, and respectful in sharing our ideas and thoughts, and in receiving input.

Diversity: Microsoft promotes and supports a diverse workforce at all levels of the company. It is our belief that creating a work environment that enables us to attract, retain, and fully engage diverse talents leads to enhanced innovation and creativity in our products and services.

Equal Employment Opportunity: Microsoft promotes a cooperative and productive work environment by supporting the cultural and ethnic diversity of its workforce and is committed to providing equal employment opportunity to all qualified employees and applicants. We do not unlawfully discriminate on the basis of race, color, sex, sexual orientation, religion, national origin, marital status, age, disability, or veteran status in any personnel practice,

including recruitment, hiring, training, promotion, and discipline. We take allegations of harassment and unlawful discrimination seriously and address such concerns that are raised regarding this policy.

Safety and Health: A safe and clean work environment is important to the well-being of all Microsoft employees. Microsoft complies with applicable safety and health regulations and appropriate practices.

We are responsible, caring members of the global community.

Citizenship and Community Service: We have a strong and demonstrated commitment to the improvement of society as well as the communities we serve and in which we operate. We encourage the support of charitable, civic, educational, and cultural causes. Our contributions include cash, volunteer time, software, and technical assistance.

Respect for the Environment: Microsoft respects the environment and protects our natural resources. We comply with applicable laws and regulations regarding the use and preservation of our land, air, and water.

Microsoft's Business Conduct and Compliance Program

Administration and Enforcement

Microsoft's CELA is responsible for the overall administration of the company's Business Conduct and Compliance Program and for providing employees with resources and materials to assist them in conducting their business activities in a legal and ethical manner. In administering the program, CELA works closely with Finance, Human Resources, Internal Audit, and Security.

The General Counsel serves as the company's Chief Compliance Officer and has overall responsibility for the management of the program. The General Counsel reports directly to the CEO and, for this purpose, to the Audit Committee of the Board of Directors. The General Counsel oversees directly an Office of Legal Compliance (OLC). The Director of Compliance, who is part of the Office of Legal Compliance, reports to the Chief Compliance Officer and the Audit Committee of the Board of Directors and has the responsibility for the day-to-day administration of the Business Conduct and Compliance Program. This responsibility includes, but is not limited to, applying the Standards to specific situations in which questions may arise and interpreting the Standards in a particular situation.

The Standards of Business Conduct and the Business Conduct and Compliance Program are endorsed by and have the full support of Microsoft's Board of Directors.

Violations of Microsoft's Standards of Business Conduct cannot and will not be tolerated. Consequences for such violations may include disciplinary action up to and including termination of employment. Individuals who have willfully failed to report known violations will also be subject to disciplinary action.

Resources for Guidance and Reporting

It is your right and your responsibility to obtain guidance about a business practice or compliance issue when you are uncertain about what action you should take and to report possible violations of the Standards of Business Conduct.

If you need details on a specific policy, you may refer to the online version of the Standards of Business Conduct at <http://businessconduct> . If you need guidance regarding a business practice or compliance issue or wish to report a possible violation, talk to your direct manager, supervisor, , another member of management, your Human Resources Generalist, or your CELA contact.

You may also call the Business Conduct Line at 1-877-320-MSFT (6738). If you are calling from outside the United States, you may make a collect call to the Business Conduct Line by accessing an international operator and asking to place a collect call to 1-704-540-0139. The Business Conduct Line is a dedicated, toll-free phone line that is available to you 24 hours a day, 7 days a week, and 365 days a year. It is operated by an external third-party vendor that has trained professionals to take your calls, in confidence, and report your concerns to the Microsoft Director of Compliance for appropriate action. Your phone calls to the Business Conduct Line may be made anonymously.

If you are a Microsoft employee or vendor with access to our corporate intranet and wish to send a confidential e-mail to the Director of Compliance, you may do so by e-mailing the Business Conduct and Compliance alias buscond@microsoft.com. A confidential e-mail may be delivered via the Internet by e-mailing msft.buscond@alertline.com. These e-mails will be received by a third-party vendor, who will remove your contact information prior to forwarding a summary of the e-mail to the Office of Legal Compliance.

You may also send a letter to the Director of Compliance at Microsoft Corporation, CELA, One Microsoft Way, Redmond, WA 98052 or send a confidential fax to 1-425-705-2985. Letters and faxes sent to the Director of Compliance may be submitted anonymously if you choose to do so.

If you have a concern regarding a questionable accounting or auditing matter and wish to submit the concern confidentially or anonymously, you may do so by sending an e-mail to msft.buscond@alertline.com, calling the Business Conduct Line, or sending a letter or fax to the Director of Compliance as outlined above.

Microsoft will handle inquiries discreetly and make every effort to maintain, within the limits allowed by the law, the confidentiality of anyone requesting guidance or reporting a possible violation.

Microsoft will not tolerate any retribution or retaliation taken against any employee who has, in good faith, sought out advice or has reported a possible violation. However, if any employee makes a knowingly false report of a possible violation for the purpose of harming another individual, that employee will be subject to disciplinary action.

Our Responsibilities

All Microsoft employees are accountable and responsible for understanding and complying with the Standards of Business Conduct, applicable laws, regulations, and

Microsoft policies that are related to their jobs. In fulfilling these responsibilities each employee must:

- Read, understand, and comply with the Standards of Business Conduct, and all Microsoft policies that are related to his/her job.
- Participate in training and educational programs/events required for his/her job.
- Obtain guidance for resolving a business practice or compliance concern if he/she is uncertain about how to proceed in a situation.
- Report possible violations of the Standards of Business Conduct, policies, applicable laws, and regulatory requirements.
- Cooperate fully in any investigation.
- Make a commitment to conduct Microsoft's business with integrity and in compliance with applicable laws and regulatory requirements.

IV. MICROSOFT OFFICE GUIDELINES

General Company Guidelines

Microsoft expects all employees to exercise common sense and good judgment at all times and to act responsibly, whether or not a written policy exists regarding specific behavior. Like any company its size, Microsoft has certain expectations for employee conduct and behaviors that are based on common-sense, basic work ethics, employees' safety, and respect for others.

Microsoft expects all employees to carry out their responsibilities in a legal and ethical manner, observing both the letter and spirit of the laws under which Microsoft operates. Employees are strictly prohibited from any acts that violate the law, even if those acts are intended to benefit Microsoft. Microsoft cannot achieve its corporate goals unless it all observes these legal and ethical standards.

The following is an illustrative and non-exhaustive list of conduct and/or behavior that will not be tolerated. Any violation of the following guidelines or other misconduct may result in disciplinary action, up to and including immediate termination of employment.

- Harassment or intimidation of another person for any reason, including harassment or intimidation because of that person's sex, race, color, creed, national origin, age, veteran status, sexual orientation, disability, or religious beliefs.
- Improper use of company equipment, networks or systems.
- Any attempt to gain unauthorized access to another person's e-mail account or computer files or to any restricted area of the corporate network or corporate systems.
- Allowing non-employees access to Microsoft leased or owned property without a Microsoft authorized purpose and registration as visitors with the building receptionist.
- Loaning the employee access card or anyone else's access card to any person, including another Microsoft employee.
- Use of corporate-issued signing privileges or charge and calling cards for personal expenditures.
- Abuse of any Microsoft privilege, such as long distance phone service, postage, corporate e-mail, network systems, delivery services, free beverages, company credit cards, internal orders, access to hardware or software, etc. This includes any activity, legal or illegal, using your Microsoft position or Microsoft property, equipment or services for personal use or gain.
- Falsification or misrepresentation of company records. This includes, but is not limited to, production reports, safety reports, expense reports, application forms, benefit forms, and timecards.
- Misappropriation of company funds, property or other assets.
- Violation of the employee's nondisclosure agreement by using or disclosing confidential/proprietary information in a manner prohibited by the agreement.
- Breach of confidentiality of personnel information.
- Improper solicitation at Microsoft.
- The display, in public areas, of symbols or icons used in religious worship/ceremonies.
- Possession of explosives, firearms or other weapons on or in Microsoft leased or owned property, including company parking areas and Microsoft sponsored events. These items are also not permitted in personal vehicles being used for company business.
- Fighting or provocation that could lead to fighting.
- Removal or use of company property (except for company business), or property of other persons, without written permission.
- Intentional misuse or damage of company property or other persons' property.

- Violation of safety guidelines and/or policies that could result in injury to any person or in damage to Microsoft or personal property.
- Distribution of any literature not produced by or directly related to Microsoft business related purposes, distribution that does not comply with Microsoft policies, or distribution that does not follow Microsoft computer equipment or online system rules.
- Any activity that adversely affects the company's interests or reputation, including but not limited to, engaging in any act whether in the workplace or otherwise that, in the sole discretion of Microsoft, involves violent behavior, moral turpitude, terrorism, or which constitutes a criminal act under applicable federal, state, or local law, regardless of whether the employee is criminally charged or convicted.

Disciplinary Rules on Violations of Company Policies & Labor Discipline

A. Disciplinary Actions

All employee misconduct will result in disciplinary action. Disciplinary action is a means to educate, correct, and punish employees who violate Company Rules and Regulations, or damage the interests of Company and other employees. The main purpose of the disciplinary action is to enable employees to learn a lesson and improve in a timely manner and to enhance self-discipline for the employee, and thus to meet the Company's acceptable standards and expectations, as well as to adhere Company's principles and values. The Company has the right to terminate an employee's contract in accordance with the law for certain serious disciplinary cases.

The level of applicable disciplinary actions will be determined by the nature and seriousness of the employee's misconduct and the losses caused to the Company (including without limitations direct losses, indirect losses, and reputational losses), as well as any previous misconduct by the employee. Types of disciplinary actions include principal and supplementary disciplinary actions. The Principal Disciplinary Actions include Oral Warning, Written Warning, Final Written Warning, and Termination of Employment Contract with No Rehire. Supplementary Disciplinary Actions include enhanced training, Compensation Impact (Impact on salary raise, performance evaluation, and qualification for bonus), and Demotion. Supplementary Disciplinary Actions could be applied independently or together with Principal Disciplinary Actions: If other Company Rules and Regulations have any provisions regarding certain misconduct, the Company may discipline the employee pursuant to both this Policy and the other relevant Rules and Regulations at the same time.

The following is an illustrative and non-exhaustive list of misconduct. For circumstances not illustrated here, the Company reserves the right to take appropriate discipline actions based on the specific circumstances, nature, severity and consequences of the misconduct.

For compliance related misconduct or potential violations of compliance responsibilities and anti-corruption responsibilities, the OLC may also deviate from the disciplinary framework below to make a discipline proposal due to individual circumstances. The discipline factors for considerations include, but are not limited to, the following: (1) the seriousness of the conduct; (2) whether the conduct appears to be an isolated occurrence or part of a pattern; (3) past disciplinary history (consistent with applicable local law); (4) subject's intent or degree of culpability (e.g., intentional, knowing, reckless, or negligent conduct); (5) subject's role in the conduct (i.e., initiate, oversee, assist, obey, or fail to report); (6) subject's level of responsibility and experience; (7) the extent to which the subject cooperated in the investigation; and (8) the extent to which the subject accepted responsibility for the conduct.

The OLC is responsible for determining whether the misconduct is compliance related, conducting investigations to determine whether the facts and circumstances substantiate whether compliance violations occurred, and making the appropriate disciplinary action proposals under the OLC Compliance Discipline Framework.

Disciplinary Framework (subject to the note above related to OLC discretion in making discipline proposals):

If an employee commits the following misconduct	The Company has the right to impose the following disciplinary or non-disciplinary actions upon the employee based on the severity of the misconduct:
General violations	<p>Principal Disciplinary Actions (from more severe to less severe):</p> <ul style="list-style-type: none"> ● Written warning ● Oral warning <p>Supplementary Disciplinary Actions:</p> <ul style="list-style-type: none"> ● Enhanced Training ● Compensation Impact ● Demotion
Relatively serious violations	<p>Principal Disciplinary Actions (from more severe to less severe):</p> <ul style="list-style-type: none"> ● Final written warning ● Written warning ● Oral warning <p>Supplementary Disciplinary Actions:</p> <ul style="list-style-type: none"> ● Enhanced Training ● Compensation Impact ● Demotion
Serious violations	<p>Principal Disciplinary Actions (from more severe to less severe):</p> <ul style="list-style-type: none"> ● Immediate termination of contract and no rehire ● Final written warning ● Written warning ● Oral warning <p>Supplementary Disciplinary Actions:</p> <ul style="list-style-type: none"> ● Enhanced Training ● Compensation Impact ● Demotion

1. If an employee commits any of the following general misconduct, the company has the right to impose any disciplinary action up to and including Written Warning based on the severity of the violation.

1.1 Workplace Relationship & Safety

- Disturbing the work order in the workplace or endangering the other employees' personal or property safety, where the circumstances are minor;
- Violation of safety guidelines and/or policies, such as inappropriate use of safety equipment, refusing to obey safety guidelines, or engaging in other unsafe

- behaviors that endanger the Company, others or the employee himself or herself, but did not lead to actual harmful consequences;
 - Distributing leaflets, documents, petitions, or posting slogans which are unrelated to work on Company premises without permission;
 - Bringing persons into Company's premises without strictly follow company polices and bring risks or damages to Company.
 - Minor violations of the Anti-Harassment and Anti-Discrimination policy, including but not limited to:
 - Discriminatory and harassing behaviors of using inappropriate, mocking, discriminatory, insulting and other disrespectful languages orally or in writing in a workplace setting;
 - Harassing behaviors of less serious nature, e.g., unwelcome physical contact.
- 1.2 IT Security-Abuse of Company's Network, Facilities and Information Assets
- Unauthorized access, viewing, or posting of information or materials relating to pornographic, obscene, sexually explicit, abusive, or harassing on Company premises, or via systems or equipment of the Company.
 - Improper use of Company equipment, networks, or systems leading to minor loss to the Company.
 - Use of Company resources for personal purpose, or unauthorized use of Company resources in violation of Security Policy and Responsible Use of Technology and Microsoft's Access to Business and Non-Business Related Data or use software or services that are not approved by Microsoft to send or store business-related data, where the circumstances are minor.
 - Unauthorized use of other's computer or account.
 - Wasting or spoiling Company property, or misusing Company equipment, networks or systems, where the circumstances are minor.
- 1.3 Protection of Company Assets
- Loss of Company documents that leads to minor loss to the Company.
- 1.4 Violation of Expense Reimbursement Requirements
- Minor violation of Company's financial, travel and reimbursement policies, where no intention was found, the amount involved is no more than RMB 1,000, and no previous similar violation.
- 1.5 Conflict of Interest
- Violation of the Company's Conflict of Interest Policy causing potential conflict of interest against the Company, where no personal benefit was involved and no actual conflict was found.
- 1.6 Procurement policy
- The employee violates third party payment policy via making payments through an unauthorized vendor, but the amount involved is no more than RMB 10,000, and without any indication of fraud, bribery, or corruption.
- 1.7 Confidential information
- Loss of Company's confidential documents that may lead to a potential threat or serious damage to the Company.
- 1.8 Intellectual Property Protection
- Making copies of copyright material without authorization, including the Company's programs, for personal purpose.
 - Without authorization, distributing copyright material of the Company or a third party over an internal or external network of the Company or through other distribution or communication methods.
- 1.9 Ethical Sales
- Modifying the transaction model, providing false, fake or misleading information, or failing to timely provide the changed information to the review team when there are changes to the circumstances, in order to circumvent or

mislead any audit or review required by the company, where there is no other disciplinary violation.

1.10 Side Agreement

- The employee knows about any other employee's personal promise, side agreement or any other authorized nonstandard agreement with client, agent, vendor or other third party, but fails to report to the Company, without causing any serious losses to the company, customers, or partners.

1.11 Gifts, Entertainment, Trustworthy Representative Policies, and Other Anti-corruption Policies

- Violation of the trustworthy representative policy, which may cause economic losses of no more than RMB 1,000 to the Company, but no actual damages to the reputation of Company, Company's partners and customers, and no actual loss or risk of Company violating laws and regulations;
- Violation of Company's gift, entertainment, trustworthy representative policies or other anti-corruption policies that does not involve offering, giving, or receiving any improper transfers of value for unjustified interests or purpose, where the amount involved does not exceed RMB 1,000, or the loss caused to Company does not exceed RMB 1,000, and it causes no damages to the reputation of Company, Company's partners and customers, and no actual loss or risk of Company violating laws and regulations.

1.12 Unfair Competition

- Violation of the Fair Competition Policy or policies relating to the collection and use of competition information, resulting in a loss of no more than RMB 1,000 to Company, but no damages to the reputation of Company, Company's partners and customers, and no actual loss or risk of Company's violating laws and regulations;

1.13 Leadership/management

- The employee's direct manager does not know of the non-compliance issue of the employee due to the manager's negligence or violation of Company policies/procedures.

1.14 Others

- The employee knows about any other employee's similar misconduct which violates the Company Rules and Regulations, but fails to report to the Company.
- Violation of Company's Standards of Business Conduct, employee code of conduct or other rules and regulations during non-working hours, which also violates local social morality, public order and morals, whether it is related to work or not, but has not caused losses or adverse impact;
- Instigating, persuading, attempting to persuade, or assisting others in instigating, persuading, or attempting to persuade any person in Company (including affiliated companies) to terminate the employment or labor relations with Company (including affiliated companies) to work for or provide service to any organization or individual other than Company, but has not caused adverse impact or losses;
- Engaged in two or more misconducts that can be given Oral Warnings within 6 consecutive months.
- Any other general violations of rules and regulations with similar severity as those mentioned above.

2. If an employee commits any of the following relatively serious misconduct, the company has the right to impose any disciplinary actions up to and including Final Warning based on the severity of the violation.

2.1 Workplace Relationship & Safety

- Use improper language or behavior with intimidation, insult, defamation, or aspersion against other colleagues or employees of the clients, vendors, or

business partners, which creates a hostile work environment or Company received complaints as a result.

- Violation of safety guidelines and/or policies, such as inappropriate use of safety equipment, refusing to obey safety guidelines, or engaging in other unsafe behaviors that endanger the Company, others or the employee himself or herself, causing the Company to suffer a loss no more than RMB 10,000 but no personal injuries.
- Relatively serious violations of the Anti-Harassment and Anti-Discrimination policy, including but not limited to:
 - Using threatening, insulting, defamatory or slanderous or other improper languages or behaviors towards other colleagues of the Company or employees of customers, suppliers, or partners, resulting in a hateful or hostile working environment or being complained.
 - Other relatively serious violations of the Anti-Harassment and Anti-Discrimination policy.

2.2 IT Security-Abuse of Company's Network, Facilities and Information Assets

- Violations of Company policies on Company system, network, e-mail, chat and text message usage, causing system or communication malfunction.
- Unauthorized or unapproved access or use of data or information (no matter whether it is protected or not).
- Assessing, modifying, damaging, defacing, moving, copying or destroying data which belong to other persons without their consent or prior authorization.
- Loading any Company IT data onto any personal electronic device/storage system without authorization or prior approval (such as personal mobile phone or email).
- Misrepresenting in the name of others or through other's email account, computer, or other Company assets without causing any damages to the Company or others or causing a loss of no more than RMB 10,000 to the Company or others.
- Usage of software not officially authorized by Company on the Company owned computers or the usage of the Company licensed software on non-Company owned IT device without causing any damages to the Company or others or causing a loss of no more than RMB 10,000 to the Company or others.

2.3 Company Assets Protection

- Dereliction of duty, carelessness, or negligence that results in loss, leakage, or damages to Company information and data, causing loss to the Company not exceeding RMB 10,000.
- Leakage of Company related information or incorrect comments to the Company through media, network, or other communication tools without permission and in violation of Company policy, where the circumstances are not serious.
- Providing a Company badge or other cards that provide access to the Company's office area and system to others, or to provide or leak electronic account username and password to others.

2.4 Violation of Expense Reimbursement Requirements, authorization and approval procedures

- Violation of Company's financial, travel and reimbursement policies where the violator was found to have the intention to do so, but without evidence of fraud or corruption. Or if the amount at issue exceeds RMB 1,000 but does not exceed RMB 10,000, regardless of whether intent to violate Company's expense reimbursement requires was found. If the employee commits a second violation of Company's expense reimbursement requirements, regardless of the amount at issue or whether intent was found, the Company may give a final written warning to the employee.
- Violation of the Company's authorization management procedures, without causing economic loss to the Company or the loss does not exceed RMB 10,000.

- Signing a contract or agreement using the name of the Company without pre-approval, without causing economic loss to the Company or the loss does not exceed RMB 10,000.
- 2.5 Confidential Information
- Loss of Company's confidential documents that led to an economic loss of no more than RMB 10,000 to the Company.
- 2.6 Violations Relating to Partners
- ECIF PO owner fails to discover the business partner's noncompliance issue of falsification or inflated charge in BIF project as a result of violation of Company policies or procedures, or fails to report the noncompliance issue while being aware of it or shall be aware of it.
 - MDF PO owner fails to discover the business partner's noncompliance issue of falsification or inflated charge in MDF project as a result of violation of Company's Rules and Regulations, or fails to report the noncompliance issue while being aware of it or shall be aware of it.
 - Microsoft account owner fails to discover pre-loading/channel stuffing issue of business partner as a result of violation of Company policies or procedures, or fails to report such issue while being aware of it or shall be aware of it. (A "pre-loading/channel stuffing issue" in this paragraph refers to a software and service vendor's submission of purchase order to the Company before the vendor has signed true and valid contract with the ultimate user.)
 - Microsoft employee fails to discover the business partner's noncompliance issue of defrauding for sales awards via providing false information or documents (which is non-compliant with Microsoft policies) due to a violation of Company policies or procedures, or fails to report the noncompliance issue while being aware of it or shall be aware of it.
 - Microsoft employee fails to discover the business partner's other noncompliance behaviors which violate the Company policies or procedures due to a violation of Company policies or procedures, or fails to report the noncompliance issue while being aware of it or shall be aware of it.
- 2.7 Ethical Sales
- Modifying the transaction model, providing false, fake or misleading information, or failing to provide the changed information according to review or risk control procedures when there are changes to the circumstances, in order to circumvent or mislead any review or examination required by the Company, and meanwhile a general violation is committed.
- 2.8 Gifts, Entertainment, Trustworthy Representative Policies, and Other Anti-corruption Policies
- Violation of Company's gift, entertainment, trustworthy representative policies or other anti-corruption policies, that does not involve offering, giving, or receiving any improper transfers of value for unjustified interests and purpose (i.e., no bribery or corruption is constituted), but the amount involved exceeded RMB 1,000, the loss caused to Company exceeded RMB 1,000, or it goes against Company's values and may cause damages to the reputation of Company, Company's partners and customers, or loss or risk of Company's violation of laws and regulations.
- 2.9 Unfair Competition
- Interference with indirect sales model by sales personnel, including but not limited to involving in trade pricing that affects business partners, affecting user's selection of business partner, such as leveraging LOAs, discount, marketing dollar, or BIF, without causing any losses to the Company.
 - Violation of the Fair Competition Policy or policies relating to the collection and use of competition information, resulting in a loss of more than RMB 1,000 to Company, or it goes against Company's values and may cause damages to the

reputation of Company, Company's partners and customers, or actual loss or risk of Company's violation of laws and regulations;

2.10 Leadership/Management

- Company's management or immediate manager does not stop subordinates' violation of the Company's Rules and Regulations or work procedures and policies which s/he observed or known or s/he should have known, in a timely manner, and allow the misconduct to continue.

2.11 Others

- Posting or distributing seditious documents or images inconsistent with the Company's Rules and Regulations, which damages other employees, Company's reputation or government's image, or harms public order and morals.
- Absent from work for less than 3 consecutive working days (not including) or less than 5 accumulative working days (not including) in 12 months (absence from work for less than an entire working day will be calculated accumulatively, any absence less than 4 hours will be counted as half a day and any absence more than 4 hours but less than 8 hours will be counted as 1 day) without reasonable justification.
- Refusing to carry out immediate manager or other higher-level managers' work assignment without reasonable reasons, even after admonishment.
- Any carelessness, negligence, or intentional action that lead to financial loss to the Company up to RMB 10,000.
- Engaged in two or more misconduct that can be given written warning within 6 consecutive months.
- Any other relatively serious misconduct with similar severity as those listed above.

3. If an employee commits any of the following serious misconduct, the company has the right to impose disciplinary actions up to and including immediate termination of labor contract with no rehire depending on the severity of the violation.

3.1 Workplace Relationship & Safety

- Any act that creates a hateful, hostile or unsafe work environment, including but not limited to sexual or other types of harassment, discrimination, slander, or intimidation and other serious violations of Anti-Harassment and Anti-Discrimination Policy.
- Violence in the workplace, such as fighting, or provocation that could lead to fighting on the Company premises, which leads to significant impact on the safety of colleagues and working areas.
- Violation of safety policies, such as improper use of safety facilities, refusing to obey safety guidelines, or other unsafe behaviors that endanger the Company, others, or the employee himself or herself, causing loss in the amount of RMB 10,000 or above to the Company or causing personal injury.

3.2 IT Security-Abuse of Company's Network, Facilities and Information Assets

- Uploading or downloading material, information or other document that is illegal, in violation of the Company's Rules and Regulations, or violates national or local laws;
- Disseminating illegal information or materials including those relating to pornography, obscenity or amateness in the Company's workplace or using the Company's systems or equipment to do so, which has caused material impact on the safety of colleagues and the workplace;
- Changing the configuration of IT device through modification or removal of hardware or by adding hardware to IT device without the permission of the IT department;
- Usage of software not officially authorized by Company on the Company owned computers or the usage of the Company licensed software on non-Company owned IT device, which causes economic loss in the amount of RMB 10,000 or above or damage to the Company's reputation;

- Opening suspicious emails or relevant attachments without being sufficiently vigilant, causing Company's network or a certain business site to be infected with virus.
- Improper use of Company equipment, networks, or systems causing an economic loss of RMB 10,000 or above to the Company.
- Posing as another person or using other people's email account, computer or other Company assets to make false statements, causing economic loss in the amount of RMB 10,000 or above or damage to the reputation of the Company or the employee.
- Maliciously encroaching on Company's network, work or electronic communication system and causing malfunction, including but not limited to attacking the security of the system; releasing a virus or other program which damages the system or the network.
- Using the system or device of the Company to conduct activities that harm the security and interest of the Company or the country.

3.3 Company Asset Protection

- Unauthorized possession, control, and use of the Company seal (including photocopy and electronic forms of the Company seal) or Company's finance, tax, or other business operation documents.
- Serious waste of, or improper use of company equipment, networks, or systems, which causes serious financial losses in the amount of RMB10,000 or above to the Company.
- Leaking information related to the Company to the media, internet, or other mass media without prior permission, or slander, insult, spread a rumor of, asperse the Company by a media outlet, internet or other mass media which causes economic losses in the amount of RMB10,000 or above to the Company or damage to the Company's reputation.
- Stealing, embezzling, or misappropriating properties or assets of Company, clients, or other employees.
- Intentionally or negligently causing loss, disclosure, or damage to Company information and data, which results in damage to the reputation of the Company or economic loss to the Company in the amount of RMB 10,000 or above.

3.4 Violation of Expense Reimbursement Requirements, authorization and approval procedures

- Committing fraud in the application for loan from the Company or expense reimbursement (including but not limited to submitting false reimbursement application or supporting documents, or submitting fraudulent facts related to expenses or expense amount or make false representations on the usage or purpose of the expense) regardless of the amount at issue. Or if the amount at issue exceeds RMB 10,000, regardless of whether there was evidence of fraud or intent to violate Company's expense reimbursement requirements. If the employee commits a third violation of Company's expense reimbursement requirements, regardless of the amount at issue or whether evidence of fraud or intent to violate Company's expense reimbursement requirements was found, the Company may immediately terminate the employee's employment contract with no rehire.
- Failure to report to direct manager in a timely manner the problem, damage, incident, etc. in accordance with policies, which results in delays in working schedule required by relevant regulations or by the Company or delays in work progress or leads the Company to assume possible legal liability or other significant adverse impact on work.
- Violation of the Company's authorization or approval procedures causing economic loss in the amount of RMB 10,000 or above to the Company or damage to the Company's reputation.
- Signed a contract or agreement using the name of the Company without pre-approval causing economic loss in the amount of RMB 10,000 or above to the Company or damage to the Company's reputation.

3.5 Procurement Policy

- The employee violates third party payment policy via making payments through unauthorized vendor, involving amount of RMB 10,000 or above.

3.6 Conflict of Interest and Violation of Outside Work Policy

- Violation of the Company's Conflict of Interest Policy, where actual conflict was found, or direct or indirect personal benefit resulted from such acts.
- Using personal influence to influence or cause the Company to do business with a company, institution, or person where the employee, the employee's family members, or the employee's friends may benefit.
- Without prior written approval from the Company, directly or indirectly engaging in one's own business or work full-time or part-time for other companies during working time or doing so by using the Company's resources (including material resources and social network resources).
- Violation of the Company's Conflict of Interest policy or Outside Work policy, engaging in part-time activities with conflict of interest during the employment period without approval, or working for any of the Company's (including affiliates) competitors (whether as an investor, partner, employee, consultant, contractor, agent or other roles), or directly or indirectly providing services to such competitors, or in any self-employed way engaging in business or production activities directly or indirectly competing with the Company's (including its affiliates) business.
- Establishing labor relations with other employers during the performance of the labor contract with Company, which has a serious impact on the completion of the Company's work tasks, or refusing to make corrections as required by the Company.

3.7 Confidential Information

- Loss of the Company's confidential documents, causing adverse impact on Company or economic loss in the amount of RMB 10,000 or above to the Company.
- In breach of the confidentiality obligations, revealing Company's confidential or proprietary information or trade secrets or using such information beyond job responsibility (no matter on purpose or not), or revealing or using the confidential or proprietary information or trade secrets of former employer or any other third parties.

3.8 Intellectual Property Protection

- Making copies of the Company's copyright material without authorization, including the Company's programs, and providing them to third parties for reproduction, use, transmission or sales.
- Without authorization, distributing copyright material of the Company or a third party over an internal or external network of the Company or through other distribution or communication methods, causing economic or reputational losses to the Company.

3.9 Ethical Sales

- Modifying the transaction model, providing false, fake or misleading information, or failing to provide the changed information to the review team when there are changes to the circumstances, in order to circumvent or mislead any review or examination required by the Company, and meanwhile other serious violation was found.

3.10 Gifts, entertainment, trustworthy representative policies, and other anti-corruption policies

- Violation of Company's gift, entertainment, trustworthy representative policies or other anti-corruption policies that although does not involve offering, giving, or receiving any improper transfers of value, the amount involved exceeds RMB 10,000, or the loss caused to Company exceeds RMB 10,000, or it seriously violates Company's values and caused damages to the reputation of Company,

the reputation of Company's partners and customers, or actual loss or risk of Company's violation of laws and regulations.

- Offering or giving anything of value (including but not limited to cash, cash equivalents (such as shopping cards or gift cards), gifts, treatment, or any other interest) to individuals, departments, or groups (including but not limited to government departments, officials, or trading counterparties) for the purpose of obtaining, maintaining business, or acquiring an improper benefit; asking for receiving those things of value, treatment or any other interests from third parties (including colleagues);
- Unauthorized business activities without obtaining pre-approval under the Microsoft Anti-Corruption Policy or the Microsoft China Policy on Gift, Entertainment, Travel Sponsorship, and Charitable Donations. Moreover, the business activities and underlying expenses in question would not have been approved if applied.
- Violations of, or causing, or instigating others to violate Microsoft's Anti-Corruption Policy, Procedure for Hiring Decisions Involving Government Officials, Trustworthy Representative Policy or the Microsoft China Policy on Gift, Entertainment, Travel Sponsorship, and Charitable Donations.
- All misconduct that violates Microsoft Code of Business Conduct, including but not limited to the following items:
 - Receiving kickbacks (or rebates, commissions, or other things of value, regardless of their name) from vendors, distributors, agents, or consultants, etc.
 - Providing Microsoft documents inappropriately to vendors, distributors, agents and any other entities or persons, to plan or commit fraud, or facilitate or assist the entities or persons to commit fraud.
 - Any trading with vendors, customers, agents, distributors at the expense of the Company's interests.
 - Other behaviors that violate Microsoft code of business conduct and PRC Anti-Unfair Competition Law.

3.11 Dereliction of Duty

- Serious dereliction of duty, including but not limited to failure to perform job responsibilities or negligence during the performance of duties, failure to perform the supervisory or audit responsibilities by employees with those responsibilities, or failure to strictly follow the Company's Rules and Regulations or job specification, that results in economic loss to the Company in the amount of RMB10,000 or above, or adverse impact on the Company's reputation, or personal injury to an employee or other person.

3.12 Fraud and Malpractice

- Fraud and malpractice, including but not limited to using or overstepping his or her authority, or violation of Company operational processes or procedures, or to use Company assets, equipment, or other resources, to gain personal benefits or for purposes other than performance of duties, that result in economic loss to the Company in the amount of RMB 10,000 or more.

3.13 Side Agreement

- Using, drafting, signing, offering, promising, or approving a side agreement or any other unauthorized, non-standard agreement, which caused economic or reputational losses to Company, Company's clients or partners.

3.14 Failure to Cooperate with Company's Investigation

- Interference with or obstruction of compliance investigations, provide false or misleading information or leave out important information during the internal investigation, not answering questions posed by investigators, coordinating statements of witnesses, intimidation of witnesses, making or instigating others to make false statements, or submission of fabricated or altered evidence; deleting any data from company devices potentially related to an investigation, deleting company-related data from personal devices.

3.15 Violations Relating to Partners

- ECIF PO owner participates in noncompliance issues such as falsification or inflated charge that occur in the BIF project that the BIF PO owner manages.
- MDF PO owner participates in noncompliance issues such as falsification or inflated charge that occur in the market activities that the MDF PO owner manages.
- Where the business partner has pre-loading/channel stuffing issue, and the MS sales managing this account participates in such noncompliance issue or pressured the business partner which led to such noncompliance issue.
- Where the business partner used a fake seal or committed other illegal acts, and the MS sales managing the project participated in or pressured the business partner which led to such illegal acts.
- MS sales personnel involved in the business partner's noncompliance issue of misusing sales awards.
- Any other similar misconduct with similar severity conducted by business partners, and MS managers participated in or actually organized to conduct such noncompliance issues.

3.16 Unfair Competition

- Interference with indirect sales model by sales personnel, including but not limited to involving in trade pricing that affects business partners, affecting user's selection of business partner, such as leveraging LOAs, discount, marketing dollar or BIF, involving an amount that exceeds RMB 10,000.
- Violation of the Fair Competition Policy or policies relating to the collection and use of competition information, resulting in a loss of more than RMB 10,000 to Company, or it seriously violates Company's values and caused damages to the reputation of Company, the reputation of Company's partners and customers, or actual loss or risk of Company's violation of laws and regulations.

3.17 Fraud and Dishonesty

- When applying for leave (including without limitations to sick leave, leaves relating to family or other leaves), providing false, forged, illegal, incomplete certificates or application materials; or failing to provide true and valid leave application materials as required by the Company within specified time; or when Company has objections to the sick leave proofs, refusing or failing to cooperate with the re-examination without justified reasons; or engaging in part-time or business activities during the sick leave; or traveling to a place of non-habitual residence for non-treatment purposes during the sick leave;
- Concealing information that has important impact on performing the employment contract, including without limitations to maintaining labor relations with any third party when signing the labor contract with Company, signing and performing the labor contract with Company may violate any contractual or legal obligations assumed by the employee (including without limitations to the non-competition, non-disclosure and non-solicitation obligations to his/her former employer) or constitute any infringement on the existing or past labor relations between the employee and any other parties.
- Altering or fabricating or destroying any records or documents related to the Company's business, management, or personal work, including but not limited to accounting and sales records, business documents, emails, and personal records.
- Organizing, planning, or implementing any fraud or deceptive action to the Company, clients, vendors, business partners, or any other Company-related organizations and individuals.
- Providing false information to the Company, including but not limited to providing any false and misleading information or intentionally concealing any important information during hiring (such as CV, education information, personal previous compensation, and benefits information, etc.), performance review, training, promotion, position adjustment, salary increase, reimbursement, market survey, and internal investigation; Providing incomplete or false information in background check or anti-corruption review during the

Company's recruitment process, including without limitations to providing incomplete or false information in filling the candidate information disclosure form.

3.18 Leadership/Management

- Supervisor and/or personnel from other functional departments take actions to retaliate against or intimidate good-faith whistleblowers.

3.19 Violations of Law/Public Regulation

- Serious violation of PRC Road Traffic Safety Laws as listed (but not limited to) below by using car owned or rented by the Company:
 - Driving without a valid driving license
 - Driving while intoxicated or under the influence of alcohol or drugs (PRC Road Traffic Safety Law shall be referred to for categories of drugs)
 - Using counterfeit vehicle license plate, or intentionally obscuring the license plate
 - Leaving the scene after causing an accident
- Violations of the law, causing criminal liability being pursued.
- Any misuse / consumption of drugs, abuse of alcohol or gambling or providing / dealing drugs in the Company's premises or within working hours or during work process or outside the Company but in the places related to the Company or Company's activities.
- Organizing or instigating strike or slowdowns or damaging the Company properties with violence and other behaviors that seriously affect the operational order of the Company.
- Possession of unauthorized guns, ammunition, and controlled weapons described in national regulations in the Company's premises or within working hours or during performing duties.

3.20 Others

- Absence from work for 3 or more consecutive working days or 5 or more accumulative working days in 12 months without reasonable justification. For clarification, failure to apply for leave according to Company's policies and procedures or taking a leave without approval and justified cause would be regarded as absence.
- Without any reasonable reasons, refusing to carry out direct manager or higher-level managers' work assignment or perform job responsibilities, or seriously violate the operation processes issued by the Company or by the business department, even after three or more admonishments, or causing economic loss to the Company in the amount of RMB 10,000 or above, or causing delays of work schedule (no matter required by the Company, third party, or other relevant policies); or the situation lasts for two weeks or more.
- Engaging in two or more misconduct that can be given final warning within 12 consecutive months.
- Making the Company enter into a labor contract in violation of its true intent through fraud, coercion, or taking advantage of its vulnerable position (fraud includes without limitations to providing incomplete or false information in the background check or anti-corruption review during the Company's recruitment process, such as providing incomplete or false information in filling the candidate information disclosure form, making false statements and warranties in the Employee Commitment, concealing or lying about academic credentials, work experience, qualifications, health status, or providing fake academic degree certificate, qualification certificate and other untruthful materials);
- Instigating, persuading, attempting to persuade, or assisting others in instigating, persuading, or attempting to persuade any person in Company (including affiliated companies) to terminate the employment or labor relations with Company (including affiliated companies) to work for or provide service to any organization or individual other than Company, and has caused adverse impact on or losses to Company;

- Violation of Company's Standards of Business Conduct, employee code of conduct or other rules and regulations during non-working hours, which also violates local social morality, public order and morals, whether it is related to work or not, and has caused losses or adverse impact on Company, society or the country;
- Violations of the Microsoft [Global Trade Compliance Policy];
- Other violations of the Company's Rules and Regulations, job documents, or the labor contract or other relevant agreements based on which the Company can terminate the labor contract, and any other particularly serious violation of laws, regulations and Company's Rules and Regulations with similar severity as those listed above.
- Any other behaviors detrimental to Company's interests or reputation, including but not limited to, engaging in any act whether in the workplace or otherwise that involves violent behavior, moral turpitude, or terrorism, or that constitutes a criminal act.
- Any dishonest actions and other serious violation behaviors with similar severity as those listed above.

The examples of serious employee misconduct listed above are not exhaustive. The Company reserves the right to take appropriate disciplinary actions for an employee's misconduct not listed above in accordance with PRC law. The Company reserves the right to discipline an employee in a manner that it deems appropriate, depending on the severity and circumstances of the misconduct. Company management team also reserves the right to exercise discretion to take disciplinary actions up to and including termination at any time that an employee is found to not follow the Code of Conduct and/or other compliance policies and procedures.

If an employee is suspected of having committed misconduct, the Company may suspend her or his work until investigation of such misconduct is complete. The employee will receive normal salary during any such period of suspension.

B. Consequences of Disciplinary Actions

For employees who are under the effective durations of disciplinary action, the wage adjustment, performance review, and eligibility for bonus award and promotion may be affected (Compensation impact) or with possibility of being demoted. The effective durations of disciplinary actions are as follows: Oral Warning: 6 months; Written Warning: 6 months; Final Written Warning: 12 months

For any employee who is given Written Warning, he or she will not be eligible for job promotion within 6 months after such a warning is given.

For any employee who is given Final Written Warning, the consequences and impacts of this disciplinary action will be EITHER:

1. Such employee will not be eligible for job promotion within 12 months after such a warning is given, and he or she will not be eligible for annual bonus for the current fiscal year and salary increase for the next fiscal year; or
2. Such employee will be downgraded according to relevant Company rules, and the compensations will be adjusted according to the position and job grade after change.

The Company will make final decision on which action mentioned above will be taken based on the actual situation of the employees.

For any employee who seriously breaches the Company's Rules and Regulation which may lead to the disciplinary action of Termination of Employment Contract, whether her or his employment ends as a result of unilateral termination by the Company, mutual termination by the parties, resignation or expiration, he or she will not be eligible for the annual bonus of the year in which the disciplinary action takes place. If the bonus is already paid before the end of investigation and final disciplinary action decision is made, the Company has the right to

request the employee to return the bonus and deduct such bonus from the salary, severance and other amount payable to the employee.

If an employee's misconduct results in damages to the Company, he or she may be required to compensate for Company damages. If the employee refuses to compensate, the Company may claim damages against him or her through any available legal remedies, including but not limited to deduction from employee's salary, bonus, reimbursement, severance pay, and other payments due to the employee.

If an employee is on leave when his/her labor contract was terminated for serious violation of Company Rules and Regulations, the employee should immediately stop the leave after receiving Company's notification of termination.

For the employees who seriously violate the Rules and Regulations and receive the disciplinary action as termination of employment contract, within the extent allowed by law, the Company reserves the following rights:

- Internally announcing the gross misconduct committed by the employee within the Company and using such gross misconduct as case study material in the Company internal compliance training.
- Not to rehire the employee in future.
- Responding truthfully, such as "the Company will not consider rehiring the employee", when a third party asks the Company for reference check.
- Consider transferring the case to government authorities for further actions

C. Service of disciplinary action decision

The disciplinary action decision will be notified in writing to the employee during the interview with him/her, and meanwhile delivered to the employee in writing through the contact information provided by the employee, including but not limited to mail, courier, telephone, SMS, e-mail, and WeChat, etc., all of which are effective. The disciplinary action decision served by the Company according to the contact information provided by employee shall be deemed to have been served to the employee and the employee is aware of it. If any contact information of an employee changes, the employee must notify the Company to change the information within three (3) working days from the date of the change. If the employee fails to notify the Company in time, the Company may serve the decision according to the contact information before the change, and it shall be deemed as effective. If the Company is unable to serve the disciplinary action decision or notice of contract termination or other related documents to the employee in time due to the employee's failure to sign for receipt or refusal to cooperate or other reasons of the employee, the employee shall bear the corresponding legal liabilities, and compensate the Company for possible losses.

More information about this policy, please read HR Policy #703 - Employee Discipline Policy and Discipline Action on Violations of Company Policies
(<https://microsoft.sharepoint.com/sites/HRweb/SitePages/hrpolicy703.aspx>)

Information Technology Guidelines and Policy

Online Systems

Employees' use of information technology and access to its contents are authorized for legitimate Microsoft work-related purposes. At all times, employees are expected to use good judgment and common sense and to conduct themselves ethically and professionally in accessing and using company-provided information technology and its contents. Violation of this policy or any operational procedures or guidelines developed in support of it, or any other misuse of Microsoft's information technology or its contents may result in disciplinary action, up to and including immediate termination of employment, and may also result in legal action.

Microsoft's various IT systems (for example: email, corporate networks, servers and Intranet, Internet connections, telephone, fax, electronic bulletin boards, public folders, remote access services, and or any other online services, systems or resources) are vital business resources for providing efficient communication and information exchange pertinent to the conduct of Microsoft's business. Microsoft expects that easy access to tools and information will be used to achieve work-related goals and objectives.

Microsoft strictly prohibits the access, viewing, posting, downloading, storing, transmitting, sharing, printing, distribution, or solicitation of any information or material from any source that the company deems pornographic, obscene, sexually explicit, abusive, harassing, or otherwise offensive or inappropriate for the workplace. (E.g. images, jokes, or cartoons) This policy applies to any such activity involving the use of any company-owned or leased property, including any company-provided computer system, equipment, network access, internet access, and remote access services.

Employees may not use Microsoft's IT systems for any illegal purpose, in violation of any company policy, or in a manner that conflicts or undermines the legitimate business interests of the company. Forgery or tampering with Microsoft online systems is also prohibited.

Additional examples of conduct that will not be tolerated include, without limitation:

- Intentionally impersonating someone else, misrepresenting the origin of a communication, and/or misrepresenting yourself through the use of another's email account, computer or other Microsoft asset. This includes fabricating a message and/or sender of a message, or modifying the internal mail transport header to forge a routing path that a message takes through the Internet.
- Using another's computer without permission, for deceptive purposes, or in violation of company policy.
- Sharing your account or network access privileges with others or allowing others, including guests or family members' access to Microsoft's corporate network.
- Intentionally bypassing security mechanisms of Microsoft's corporate network or systems without authorization (such as by creating bogus accounts, creating non-OTG approved and managed remote access points into Microsoft's corporate network, and the use of non-corporate security approved peer-to-peer (P2P) network sharing software on systems connected to the corporate network).

This policy extends to the worldwide corporate network, related online systems and interconnections to other networks and information systems of which Microsoft has management and control. All protection standards are equally applicable to the digital data streams, stored digital data, hard copy, video image and sound generated from the physical resources of the network.

Employees may use Microsoft's IT systems for the following incidental personal uses so long as such use does not interfere with the employee's work duties, is not done for monetary gain, and does not conflict with Microsoft's legitimate business interests, or otherwise violate any company policy:

- To send and receive occasional personal communications
- To prepare and store incidental personal data (such as personal calendars, personal address lists, and similar personal data) in a reasonable manner

In order to promote the efficiency and security of the electronic communication system and

avoid the disruptions caused by "spamming," Microsoft prohibits non-work related mass emails, voicemails or multiple distributions to employees or others as incidental personal uses of the online systems. "Mass emails/voicemails" or "multiple distributions" are defined as sending the same or substantially the same personal communication to five (5) or more recipients.

The corporate network, all its components and contents, as well as any other data stored on or transmitted by Microsoft equipment, are the property of Microsoft. Employees should understand that they have no right of privacy with respect to any messages or information created, sent, or maintained on Microsoft's IT systems, including what might be thought to be personal messages. The company may, at its discretion, inspect and monitor all files or messages on its IT systems at any time for any reason. In particular, Microsoft may monitor its IT systems at any time to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

Connections to external services outside Microsoft corporate network are strictly prohibited unless accomplished through OTG-engineered approved mechanisms. (see: <http://itweb/security>)

It is the responsibility of all authorized users to ensure the information and/or data that they create, or that is entrusted to their care, is protected using any and all physical and logical security controls that are provided, authorized and supported by the company. In addition, all authorized users of the Microsoft Corporate Network are responsible for protecting the information it contains from unauthorized disclosure, destruction, alteration or modification. Adherence to established information security guidelines, policies and procedures is a condition of employment. Additional detailed information regarding Microsoft's information security policies can be found at the internal web site <http://itweb/security>.

Online Services

Use of the corporate email account may give the appearance that the employee represents Microsoft. If the employee wishes to engage in promotion or discussion of personal, political, financial, commercial, social, or religious views, he/she needs to do so on non-work time with his/her own personal email account and equipment, and not to other Microsoft user accounts. In those instances the employee should avoid commenting on any Microsoft policies, issues, products, etc., but if the employee does so comment and his/her Microsoft employment is known, the employee should indicate that he/she is expressing solely his/her own personal views and not those of Microsoft.

All internal communications (emails, memoranda etc.) are intended for internal use only and are not for distribution outside of Microsoft. Where legitimate business needs call for distribution of internal communication outside the company, appropriate authorization from location CELA team should first be obtained.

Public folders, electronic bulletin boards and the Community Pages section of the Microsoft internal web are provided as a courtesy to Microsoft employees. These amenities are for occasional use and may be discontinued if used excessively or abused, if business need precludes their continued operation, or if at any time Microsoft determines in its discretion to discontinue them based on its assessment of legitimate business reasons. Such IT systems may not be used at any time for electronic communications by or with parties outside of Microsoft, except for Microsoft business related purposes.

It is the employee's responsibility to read and comply with the security policies located on

<http://itweb/security>. An email alias is provided within each policy for answering or clarifying any questions the employee may have.

Duty to guard against viruses

All Microsoft employees must take the corresponding responsibility for any documents, data and magnetic disks that they own or have obtained through any channel to ensure that.

- All anti-virus protection tools provided and distributed by OTG are appropriately used;
- All magnetic disks (including network drives), floppy disks and other disks under a person's control are regularly scanned for viruses;
- Before sending an e mail, a virus scan is performed on the document that will be sent as an attachment to the email;
- Any magnetic disk/attachment from an external source is scanned for viruses before opening it and disseminating it internally;

Employees must be on the alert and must not open any suspicious e mail or its attachment. It should be noted that an e mail is not necessarily made safe by not opening its attachment. Some e mails spread a virus as soon as they are opened. Therefore the most correct rule of conduct should be to immediately delete a suspicious e mail upon receiving it.

The address of Microsoft's only anti-virus web site is <http://itweb/security/antivirus>. This web site provides the latest relevant information on malicious viruses and virus code updates.

Microsoft reserves the right to take punitive action against an employee who fails to perform this duty and whose failure to do so results in a serious virus infection of Microsoft's network or of a particular operating station.

Confidential /Proprietary Information or Trade Secret

Virtually every employee at Microsoft creates, uses and/or has contact with confidential proprietary information or trade secret in the course of doing his/her job. It is included in documents and email, exchanged in telephone and hallway conversations and discussed in meetings. As part of the employee's employment with Microsoft, the employee signs a non-disclosure agreement that obligates him/her to protect confidential / proprietary information or trade secret. For the success of Microsoft business, and in order to preserve all of its legal rights to the company's proprietary information, it is imperative that all employees strictly comply with that agreement and exercise the utmost care in protecting confidential/proprietary information or trade secret.

For purposes of this Policy, "Microsoft Confidential/Proprietary Information or Trade Secret" is data and information that is not known by the general public, presented in any form and relates to the business, technology, practice, products, markets, sales, services, financial or legal affairs of Microsoft or its affiliates or any third party that has business relationship with or provide information to Microsoft or its affiliates, whether tangible or intangible, whether explicitly designated or marked "confidential" or "proprietary." , including but not limited to: information relating to actual or potential customers, suppliers and business partners; non-public information on employees, such as contact information, job responsibilities or description, remunerations and performance; commercial, business, sales, marketing, promotional, technical, financial and legal plans, strategies, recommendations and forecasts; concepts, know-how, process, approaches, systems, design, competitive intelligence, computer programs, coding, formulas, researches, techniques, technical features, experimental work and work-in-

progress; source code, pre-release builds, technical know-how, product plans, specifications, milestones, usability surveys, test results, bug data,

The employee may not disclose Microsoft Confidential/Proprietary Information or Trade Secret outside of Microsoft unless there is a compelling business need to do so and either (1) the disclosure is protected by a non-disclosure agreement or (2) the employee has obtained Director or General Manager level or higher approval for the disclosure. In addition, at all times the employee must take reasonable steps to protect Microsoft Confidential/Proprietary Information or Trade Secret.

This means, for example:

- Do not share any Microsoft Confidential/Proprietary Information or Trade Secret with friends or family members.
- Discuss Microsoft Confidential/Proprietary Information or Trade Secret with other employees only on a need-to-know basis.
- Restrict access to Microsoft Confidential/Proprietary Information or Trade Secret posted on shared internal resources such as intranet and SharePoint sites.
- Do not discuss Microsoft Confidential/Proprietary Information or Trade Secret in public places where third parties may overhear, including company cafeterias and non-secure hallways and lobbies.
- Erase information on whiteboards at the conclusion of meetings.
- Do not work with documents containing Microsoft Confidential/Proprietary Information or Trade Secret either in hard copy or using your laptop) in public places if third parties might see the information contained in them.
- Practice secure computing in accordance with IT policies.

The employee is also obligated to protect third-party confidential/proprietary information or trade secret, which should not be disclosed without the third party's consent.

For example:

- The employee may not disclose confidential/proprietary information or trade secret of a former employer.
- The employee may not induce colleagues to disclose confidential/proprietary information or trade secret of a former employer or use any confidential/proprietary information or trade secret inadvertently provided by a colleague about a former employer.
- The employee must use the same efforts to protect third-party Confidential/Proprietary Information or Trade as he/she would to protect Microsoft Confidential/Proprietary Information or Trade.
- The employee must contact CELA immediately if he/she believes third-party confidential/proprietary information or trade secret has been improperly introduced to Microsoft.

If an employee has any questions about this policy, please contact the location CELA team. The employee may not deviate from this policy without CELA authorization.

Failure to comply with this policy may lead to disciplinary action up to and including termination of employment. Unauthorized disclosure of confidential/proprietary information or trade secret may also lead to civil liability or criminal prosecution.

How Should Employee Protect Microsoft's Property – Intellectual Property

1. How should I write an e-mail to legal?

If you encounter a legal issue in your work and need to communicate it to Microsoft's attorney, we offer the following pointers, which you should follow:

- 1.1 Please use "Attorney/Client Privilege" in the subject line or at the beginning of the email or both in your email seeking legal advice from your attorney or discussing sensitive issues, and
- 1.2 Your e-mail should be addressed to the attorney. If you need to copy someone else, your manager for example, you should list that person in the "Cc" section, and
- 1.3 Never copy anyone outside Microsoft on any e-mail exchange between you and legal, and
- 1.4 Do not interpret or re-paraphrase legal advice or legal opinions and also do not forward the email to third parties including Ms colleagues.
- 1.5 Do not discuss legal issues with your colleagues in your e-mails, and especially do not draw any legal conclusions. For example, you should not make any judgments or reach any conclusions as to whether a certain technology infringes another's patent.

2. How should I protect Microsoft's copyrights?

- 2.1 First, you should not use anything other than Microsoft materials in your work.
- 2.2 Under the provisions of the Standards of Business Conduct, Microsoft employees may not use any third party materials, including third party software, games, music, images, etc., that have been pirated or for which the appropriate license has not been obtained. Failure to abide by these Standards will result in the punishment of the relevant personnel member(s), including termination of the employment.

3. How should I protect Microsoft's patents?

Under the patent laws of most countries, "novelty", "non-obviousness" and "utility" are conditions for obtaining patents. Accordingly, everyone should adhere to the following in their work:

- 3.1 Before a patent is obtained for your technology, do not discuss your technology with a third party unless they have signed a confidentiality agreement with Microsoft. Do not discuss your technology in the presence of many people, even if they have signed confidentiality agreements with Microsoft. Do not publish or disclose your patent technology on web sites, in publications or in conference materials.
- 3.2 You also must not in any way attempt to obtain the patent technology or information of another company.
- 3.3 Under Microsoft's company policy, no one may perform a patent search without

authorization. Performing a patent search requires approval from a Microsoft vice president and legal counsel.

- 3.4 You also must not make comments on Microsoft patents or third party patents.

4. How should I protect Microsoft's trade secrets?

- 4.1 Every one of us has an obligation to protect Microsoft's trade secrets. For example, we should not leave documents that contain company confidential information in unsafe places and should not discuss company confidential information in public places (hallways, elevators, restaurants, etc.). We should only disclose and discuss company confidential information on a need-to-know basis. We should cultivate the good habit of marking all documents and materials that contain company confidential information as "Microsoft confidential/proprietary information or trade secret".
- 4.2 We should also abide by the same obligation to maintain confidentiality as regards third party trade secrets. We should not use or further disclose such information to other persons, especially if we are aware that the person disclosing the confidential/proprietary information or trade secret to us has not obtained the appropriate authorization or we suspect that he/she has obtained such information through improper channels.

5. What should I do if I want to use third party components/OSS?

- 5.1 Microsoft has a strict policy concerning the use of OSS (<http://lcaweb/Open+Source/default.htm>). Please read this policy carefully.
- 5.2 Improper use of OSS may harm the company's interests. If you need to use OSS, please first obtain permission from your manager and Legal. If your request is approved, you should use OSS as stipulated.
- 5.3 Unless you have compelling reasons for doing so, you may not accept source code from a third party. Acceptance of third party source code requires signature of a written agreement with the third party.
- 5.4 You must obtain the approval of the Director to access or use third party source codes, including OSS source codes.

6. If I receive a letter from a third party with its recommendations, feedback, creative ideas or thoughts concerning Microsoft products, what should I do?

- 6.1 In order to protect Microsoft, you should not accept, read or reply to unsolicited recommendations, feedback, creative ideas or thoughts sent to you by a third party. You should delete e-mails you receive containing the same (http://msrinfo/legal/outside_materials.htm).
- 6.2 If the person making the recommendation is someone you know and a response is required for the sake of courtesy, you can use the Company's standard response script. You can also forward the email to "[prcpermi](#)".

7. Can I take third party codes into Microsoft (software)? Can I take Microsoft codes out of Microsoft (software)?

You may not bring third party codes or codes developed during the time you worked for a previous employer into Microsoft and you are not permitted to use them in your work, unless otherwise permitted by legal counsel. Pursuant to the Non Disclosure Agreement you have signed with Microsoft, the results of the work you perform during your term of employment at Microsoft are the property of Microsoft. You may not distribute the code you have developed during your term of employment with Microsoft to any outside third party without Microsoft's permission.

The above provisions are the supplement to the Standards of Business Conduct. The violation of the above provisions may result in punishment including dismissal and even criminal prosecution.

Open Source Software

"Open Source Software" or "OSS" is a topic of great interest both inside and outside Microsoft. The following material describes the proper treatment of OSS at Microsoft and supplements the policy titled "Proper Use of Microsoft and Third Party Copyrighted Material".

Additional information about OSS can be found on [CELAWEB](#). All questions relating to OSS should be directed to the location CELA team.

1) Reading, Downloading or Distributing OSS or Incorporating OSS into a Microsoft Product:

OSS is a term that is used to refer to a wide range of software products distributed under a variety of open source licenses such as the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Common Public License (CPL) and Berkeley Software Distribution (BSD) license. OSS is sometimes referred to as "publicly available" code, reflecting the fact that code released under one of the many existing OSS licenses is readily available to the public in source code form. It is important to understand, however, that such code is not in the "public domain" and is instead governed by the terms of a license agreement. Some of these licenses contain provisions that are not acceptable to Microsoft, such as warranty disclaimers, patent non-assertion clauses or requirements that Microsoft release source code or license its intellectual property under certain terms.

Accordingly, the employee is required to obtain approval from his/her location LCA team prior to undertaking any of the activities listed above. Specifically, the employee must obtain approval prior to downloading, reading, reviewing, modifying or distributing source code governed by an OSS license. The employee also must consult with his/her location LCA team prior to copying, linking to or otherwise incorporating any source or object code governed by an OSS license into a Microsoft product. More information on this approval process is located on [CELAWEB](#).

The employee may, however, obtain in executable form (i.e., non-source code form) and run internally any program that is subject to an OSS license (including the GPL or any similar license), provided that the license or agreement does not require him/her to accept additional restrictions and/or obligations as a condition of merely running the software. This exception applies only to the internal use of OSS executables, and does not allow the employee to distribute, link or otherwise combine such executables into a Microsoft product or prototype without prior CELA approval. If the employee has questions or concerns regarding the terms of a particular license

or agreement and whether such license contains any such additional terms, he/she should check with his/her location CELA team. More information on appropriate uses of executables covered by an OSS licenses can be found on [CELAWEB](#).

The employee may also obtain and review the following non-code materials without prior consultation with the location CELA team provided that he/she complies with any accompanying licenses or restrictions:

- General information about open source projects including articles and reviews;
- Books, whitepapers, architecture descriptions, project descriptions provided at websites, and development discussions conducted on the Internet.

The employee should take care to avoid any written materials that include code samples or illustrations. If the materials the employee would like to review include sample code or other instances of source code or if those materials are governed by a license, he/she should contact his/her location CELA team for assistance.

2) Releasing Microsoft code under an OSS or Shared Source license:

Releasing Microsoft code in source code form can have a significant impact on the Microsoft intellectual property within that code or product. This is true whether the employee releases the source code under an existing OSS license, one of Microsoft's Shared Source licenses or no license at all. The employee's business unit, in conjunction with his/her location CELA team, must perform (1) an IP audit and (2) a review of the proposed license terms for any source code prior to release. The employee must obtain VP-level sign off on this IP audit and license review prior to releasing any Microsoft source code. More information on the audit and approval process for releasing Microsoft code under an OSS or Shared Source license is located on [CELAWEB](#).

The employee should also understand that as used here, the term "Microsoft code" means any code (and underlying intellectual property) that the employee has written that under the terms of his/her employment agreement would belong to Microsoft (possibly including code written outside of work hours or without use of Microsoft facilities). Please email the location CELA team if the employee has any questions about whether code he/she has written belongs to Microsoft.

3) Establishment of Microsoft "Community" Projects:

The term "Community" is commonly used to refer to the development aspects of OSS, in which volunteers make contributions to a publicly available software code base. Allowing non-Microsoft employees to make contributions to a Microsoft code base that has been released under an OSS or Shared Source license (regardless of where this code base is hosted) can raise significant intellectual property concerns, including questions around ownership of such contributions. The employee's business unit- in consultation with the location CELA team - must set up a process to carefully manage the community project, insure that ownership issues are resolved and otherwise mitigate intellectual property risks associated with the community project. The employee is also required to obtain VP-level approval prior to setting up a "community" project with a Microsoft code base. More information on the approval process for setting up a community project- including details about necessary risk mitigation processes- is located on [CELAWEB](#).

4) Contribution of Microsoft code, ideas or intellectual property to an existing

OSS "Community" project or OSS product:

There are a range of existing "Community" projects that actively solicit contributions from end users, as well as other open source products that accept unsolicited bug fixes, improvements or other suggestions in source code form from end users. Contribution of Microsoft code, ideas or intellectual property to such community projects may not be made without an IP review by CELA and Senior VP-level sign off. More information on the approval process for contributing to a community project is located on [CELAWEB](#).

The employee should also understand that as used here, the term "Microsoft code, ideas or intellectual property" means any intellectual property, code or other materials that under the terms of his/her employment agreement would belong to Microsoft (possibly including code written outside of work hours or without use of Microsoft facilities). Please email the location CELA team if the employee has any questions about whether certain code or materials belong to Microsoft.

Proper Use of Microsoft and Third Party Copyrighted Materials

Excluding the download and use of Microsoft's copyrighted material (e.g., software programs) needed in the ordinary course of your employment and as used on Microsoft equipment, the unauthorized duplication and use of non-licensed copyrighted material by Microsoft employees is a violation of the copyright laws of the United States and all the other countries in which Microsoft Corporation and its subsidiaries maintain offices. Copyrighted material includes software, documentation, graphics, photographs, clipart, animations, movie/video clips, sound and music (including when MP3 encoded). Violation of copyright laws can subject employees and Microsoft to liability for significant civil and criminal penalties. In addition, Microsoft devotes considerable resources around the world to educate software users about their obligation to use and manage software properly. In order for this effort to be effective and benefit the software industry, Microsoft must lead by example.

The following practices, unless granted by a specific license or Internet site terms, are among those prohibited by this policy (including where the copyrighted material is available via the Internet (whether fee based or free)):

- Making or using copies of non-licensed copyrighted material on Microsoft owned or other computers.
- Making copies of copyrighted material, including Microsoft's programs, for your personal use, use by friends or associates.
- Distributing copyrighted material over an internal or external network.
- Providing copies of copyrighted material, including Microsoft's programs, to bulletin board services.
- Removing or distributing from Microsoft owned networks or machines, without prior written approval of the employee's immediate manager, any copyrighted material, including without limitation Microsoft beta releases, tools, utilities or objects, that Microsoft does not make commercially available.

Location IT group maintains a list of software products that have been licensed to Microsoft for network use or for use on a site-license basis. If the employee needs third-party software for his/her job, the employee needs to ask from his/her immediate manager for approval to order it. Each department that acquires third-party software is responsible for retaining proof of proper licensing of that software, such as end user license agreements, original disks and manuals, and receipts. If the employee has questions regarding the terms of any third-party

license agreement, he/she should contact the location CELA team for clarifications.

Failure to follow this policy may result in disciplinary action against the employees involved, up to and including immediate termination of employment.

Anti-Piracy Policy

The illegal distribution, sale and use of Microsoft software products result in huge losses to Microsoft. According to an industry technology indicator commonly used to measure the size of these losses, Microsoft's annual income will double if the occurrence of all types of this illegal use can be prevented.

This document contains the relevant information and procedures to assist you to take the corresponding action to prevent and stop the occurrence of the illegal distribution, sale and use of Microsoft products. Even though the personnel of the Legal Department are the persons primarily responsible for the enforcement of Microsoft intellectual property rights, nonetheless, they can do their work more effectively only with the active support of all Microsoft employees.

Microsoft employees have the following responsibilities:

- Pay close attention to and identify suspicious situations that may involve piracy that one may encounter at any time during one's daily work;
- Find out all the relevant information on suspicious situations that may involve piracy, do not arouse any unnecessary suspicion on the part of the alleged persons committing the piracy and do not create a "panic" inside the organization;
- When you realize that there is a suspicious situation that may involve piracy, you should make a full report of the essential information that you are aware of to the Legal Department as soon as possible. You can send the information you report to the mail box named "Enforce".

The legal department has the following responsibilities:

Pursue all leads, obtain sufficient information and take action against personnel involved in piracy, whether they are Microsoft Channel Partners or end users, in cases where piracy is suspected.

The Legal Department will monitor cases of piracy that directly occur in channels and will submit the relevant leads/cases concerning end users to the BSA (Business Software Alliance) so that the BSA may cooperate with the CELA to take joint action.

How Microsoft authorizes the legal use of its software:

Copyright and trademark law specifies that only Microsoft (all owners of Microsoft copyrights and trademarks) has the right to license end users to use products which have copyrights and trademarks owned by Microsoft. Microsoft primarily grants usage licenses through the following license agreements:

- The standard End User License Agreement (EULA) used in fully packaged products (licenses use by a single end user);
- The standard End User License Agreement (EULA) used in Microsoft License Paks (licenses one copy and use by a single end user);
- The standard End User License Agreement (EULA) used in Microsoft Multiple License Paks

(licenses 20 copies and use by 20 end users); and the Microsoft Variable License Pak for large customers (licenses quantity copying and use by multiple end users, under the condition that the customer accurately reports the number of copies, the number of end users and the corresponding fees paid).

- Special OEM licensing that licenses the OEM to provide sub-licensing on Microsoft products to end users that purchase the OEM's hardware products. The OEM products will also provide a standard End User License Agreement (EULA) used in Microsoft's fully packaged products permitting the purchaser to use Microsoft products as a single end user.

Anti-Harassment and Anti-Discrimination

Policy

Microsoft is committed to providing equal employment opportunity to all qualified employees and applicants. Harassment, discrimination, retaliation or intimidation on the basis of race, color, sex, sexual orientation, religion, national origin, marital status, age, disability or veteran status towards another employee or any other person (including an agency temporary, independent contractor, vendor, or supplier) is prohibited and will not be tolerated. Please refer to Anti-harassment and anti-discrimination policy

<https://microsoft.sharepoint.com/sites/HRweb/SitePages/antiharassment.aspx> .

Examples of Sexual Harassment

Sexual harassment is unwelcome verbal or physical conduct that is sexual in nature or that is directed at a person because of his or her gender. Types of sexual harassment may include: Explicit or implicit pressure for submission to unwelcome conduct as a condition of employment or employment benefit, such as promotions or pay increases, or dismissing or threatening to dismiss the employee or withholding such employment benefits if the employee rejects the unwelcome conduct.

- Creation or perpetuation of a hostile, intimidating or offensive work environment, or unreasonable interference with an employee's work performance through unwelcome verbal or physical conduct such as:
 - Making sexual advances to an employee or another person;
 - Touching an employee or another person in an unwelcome way;
 - Making sexual comments or inappropriate jokes;
 - Viewing, downloading, or sharing sexually explicit pictures, calendars, bitmaps, or cartoons;
 - Hiring vendors for entertainment at team events that involves sexually explicit or otherwise offensive attire or behavior.

Other Forms of Harassment, Discrimination,

This policy applies not only to complaints and investigations of sexual harassment and intimidation, but to all other forms of harassment, discrimination, retaliation, and intimidation based on age, race, color, sex, sexual orientation, national origin, religion, marital status, disability, and/or veteran status.

Internal Complaint Procedure

If the employee believes that he/she is experiencing harassing, discriminatory, or retaliatory behavior or is aware of any such behavior towards others, he/she should immediately:

- Notify his/her immediate manager of the behavior. Or, if the employee feels that he/she cannot talk directly to the manager, the employee should notify his/her manager's manager or location HR representative through ASKHR or Workplace Investigations Team (WIT). The employee can send his/her notification either in verbal or in writing; and
- The employee is encouraged, but not required, to identify the offensive behavior to the person engaging in the behavior and requests that it stops.

Even if the employee has addressed the issue with the person engaging in the behavior, he/she should let his/her immediate manager, the manager's manager, or location HR representative know about the situation so that Microsoft can follow up with any measures it considers appropriate. Microsoft prohibits reprisal or retaliation against employees who raise good faith concerns of discriminatory, harassing, or retaliatory behavior or provide information as part of an investigation into alleged violations of the EEO Policy.

Company Action

In applying this policy, Microsoft has zero tolerance for prohibited discrimination, harassment, or retaliation. Microsoft has:

- An internal complaint procedure set forth in the preceding section to allow an employee to raise a concern or complaint about any conduct believed to be in violation of the EEO Policy.
- HR professionals trained to promptly conduct unbiased investigations when complaints are raised. To the extent possible, employee confidentiality is maintained.
- A policy that is enforced to protect employees who complain about discrimination, harassment, or retaliation.

Each situation is reviewed on its own facts. If it is determined at the completion of an investigation that an employee has engaged in discriminatory, harassing, or retaliatory behavior in violation of company policy, the company takes appropriate measures to:

- Stop the discriminatory, harassing, or retaliatory conduct;
- Correct its effects;
- Prevent its recurrence;
- Take disciplinary action against the wrongdoer, up to and including termination.

If the employee has any questions about this policy, he/she should contact the location HR Generalist.

Company Access and Monitoring Information and Property

E-mail and its contents, voicemail, and any other data of any kind stored or transmitted by Microsoft-owned or leased equipment, is the property of Microsoft, and the company may access, monitor, intercept and/or retain this data at any time without further notice. Such data remains Microsoft property, and Microsoft retains its right to access or retrieve such data, even if the data has been transferred to equipment that is not owned or leased by Microsoft. Microsoft may also access any of its facilities or equipment (e.g., offices, desks, computers, lockers, etc.) at any time without further notice. Employees are expected to cooperate with and expedite Microsoft access to facilities and equipment when requested, and this may include promptly turning over equipment or keys to an authorized Microsoft representative, or divulging to such

representative passwords or other means for disabling employee-created security devices. Microsoft property and equipment are maintained and made available to employees for the purpose of conducting Microsoft business, and employees should not regard as private any Microsoft premises, facilities or equipment or any property or data stored on or in Microsoft's premises, facilities or equipment.

To protect its corporate network and intellectual property, Microsoft will periodically, and without notice, perform security scans of home PCs that are connected to the Microsoft corporate network. Security scans will be limited to identifying security vulnerabilities and ensuring that home PCs have the security-related tools, programs, and capabilities that Microsoft deems appropriate. Microsoft also reserves the right to access or retrieve from home PCs any data of any kind (including, but not limited to, email, documents, code, and files) that has been transmitted to a home PCs from Microsoft-owned or leased equipment. Microsoft's rights to perform security scans and access and retrieve data apply regardless of who owns the home PC. Access and retrieval may be performed without notice.

In order to provide a safe workplace and to protect Microsoft property and trade secrets, Microsoft owned and leased property may be electronically monitored, including monitoring by surveillance camera placed either inside or outside the building. Depending on building configuration or for other security related reasons, the cameras may or may not be visible. Additionally, in order to evaluate and improve customer service, Microsoft may monitor or record telephone calls of employees in customer service positions.

Conflict of Interest

All Microsoft employees are expected to act at all times in Microsoft's best interests and to exercise sound judgment unclouded by personal interests or divided loyalties. Both in performing employee duties at Microsoft and in the outside activities, the employee should avoid the occurrence or circumstance that leads to the occurrence of a conflict of interest.

A conflict of interest exists if the circumstances would lead a reasonable person to question whether the employee's motivations are aligned with Microsoft's best interests. If, for example, the employee is involved in an outside activity or have a financial or other personal interest that might interfere with his/her objectivity in performing company duties and responsibilities, the employee may have a conflict of interest.

While it is impractical to describe all situations that may create a conflict of interest, the following provides policy guidance about some of the most common conflict of interest situations:

- Use of Company Information for Private Gain
- Friends and Family Stock
- Outside Activities – Non-Profit and Civic Organizations
- Employment Outside Microsoft - Moonlighting
- Service on a Board of Directors
- Technical Advisory Boards
- Family and Romantic Relationships
- Spouses, Domestic Partners, Immediate Family Members or Relatives as Suppliers, Vendors, and Strategic Partners
- Kickbacks and Rebates by Vendors
- Gifts from Vendors or Customers
- Honorariums or any benefits directly or indirectly obtained from engagement in any private business activities with any third party

Please note that the above is not an exhaustive list of examples. There are many other situations that may also create a potential for a conflict of interest or the appearance of a conflict of interest. It is up to the employee to be aware of the potential for a conflict of interest in his/her own particular situation and to resolve the issue in accordance with this policy.

Microsoft expects its employees to promptly report any actual or potential conflict of interest to his/her immediate manager and the location HR Generalist before taking any further action related to the situation giving rise to the conflict. The business management team will advise on the appropriate means for addressing the conflict, which may include requiring the employee to remove him/herself from the conflicting situation, requiring the employee to obtain senior management level approval to engage in the activity in question, or any other resolution the team deems appropriate.

Any violation of this policy may lead to disciplinary action, up to and including immediate termination of employment.

1) Use of Company Information for Private Gain

Use of Microsoft confidential/proprietary information or trade secret that the employee obtains by reason of his/her Microsoft employment for his/her personal gain or advantage or for the gain or advantage of another is strictly prohibited.

The use or disclosure of confidential confidential/proprietary information or trade secret is prohibited by the employee's Employee Agreement. Use of confidential information for purposes of trading in Microsoft or another company's securities is addressed by Microsoft's insider trading policy.

Failure to comply with this policy may result in disciplinary action, up to and including immediate termination of employment.

2) Service on a Board of Directors of a For Profit Company

Directors owe a duty of loyalty to the company on whose board they serve. The employee should carefully consider all potential conflict of interest issues before agreeing to serve on the board of a for profit company. Employees level 67 and above must also obtain CELA approval.

Any approval granted is subject to Microsoft's periodic review and Microsoft may at any time revoke its approval. Previous approvals are no guarantee that future approvals will be granted. Under no circumstances may a Microsoft employee serve on the audit committee for another company's board of directors.

If the employee's position on the board of directors of another company becomes potentially relevant to a Microsoft decision or action, the employee must promptly disclose his/her relationship with the other company to the Microsoft employees responsible for the decision or action and the employee must not participate in that decision or action on behalf of either Microsoft or the other company. For example, if the employee's Microsoft business unit is considering a transaction with the company on whose board the employee serves, the employee must disclose his/her relationship with the other company to the decision makers in his/her business unit and the employee must refrain from any discussions about or involvement in the transaction on behalf of either Microsoft or the other company.

Any employee considering service on another company's board should understand that such service can lead to personal liability, particularly with financially troubled companies. As the employee's board service is outside the scope of the employment, Microsoft will not defend or indemnify its employee if he/she is sued in his/her capacity as a board member of another company. Microsoft's approval of its employee's request to serve on an outside board does not constitute any endorsement or ratification of any action the employee takes as a board member of another company.

Failure to comply with this policy may lead to disciplinary action, up to and including immediate termination of employment.

Microsoft may at times ask an employee to serve on the board of directors of a for-profit organization pursuant to a Microsoft investment in, or strategic partnership with, that organization. Microsoft may also request that an employee serve on the board of a non-profit organization, such as a standards body. Service on such boards as a representative of Microsoft is outside the scope of this policy.

3) Technical Advisory Boards

Before accepting appointment to or service on a technical advisory board for a company other than Microsoft, the employee should consider whether the entity is offering him/her this opportunity in order to leverage the relationship with Microsoft to gain a special advantage for itself with Microsoft, whether serving on this board will interfere with the employee's ability to exercise his/her independent judgment in the best interest of Microsoft, and whether the products and technologies the employee works on at Microsoft are so similar to those of the company on whose board he/she wishes to serve that it would be difficult to serve as a technical advisor without using or disclosing Microsoft confidential/proprietary information or trade secret.

If, after considering these questions, the employee still wishes to serve on the technical advisory board, the employee must obtain prior written approval from his/her manager.

If any decision is to be made or action taken by Microsoft concerning a company for which the employee serves as a member of a technical advisory board, the employee must disclose to the Microsoft employees responsible for the decision or action his/her relationship to the entity and not participate in that decision or action on behalf of either party.

Employees who are asked by Microsoft to serve on a technical advisory board of another company as part of their Microsoft job duties are not required to obtain approval under this policy.

Failure to comply with this policy may result in disciplinary action, up to and including immediate termination of employment.

4) Outside Activities – Non-Profit and Civic Organizations

Microsoft encourages its employees to be active in their communities and to volunteer their time to bona fide charitable, educational, civic, and trade organizations, provided of course that such activities do not detract from their job performance. Participation in these types of activities does not generally require prior approval.

In taking on outside obligations, however, the employee should guard against possible conflicts of interest or the appearance of such conflicts. If participation in an outside activity has the potential to cloud the employee's judgment, prevent the employee from acting in Microsoft's best interests, or create an appearance that the employee will not act objectively, the employee must refrain from participation in the activity unless he/she obtains prior written approval through the conflict of interest review process.

The employee must also honor his/her non-disclosure obligation in all his/her outside activities. If an outside organization's interests are so closely related to his/her work at Microsoft that the employee might inadvertently use or disclose Microsoft confidential information in the course of that outside work, the employee must not participate in the organization.

If the employee is affiliated with a non-profit organization that is pursuing the same goals as Microsoft or goals that conflict with Microsoft's, and the employee participates in a Microsoft decision that implicates those goals, the employee must disclose at the earliest opportunity his/her affiliation with the non-profit organization and the nature of the potential conflict to the other Microsoft employees responsible for making the decision and to his/her immediate manager.

Employees who are asked by Microsoft to serve on the board of non-profit software industry organizations, such as public standards bodies, as part of their Microsoft job duties are not required to obtain conflict of interest review.

Rules for the Use of E-mail and the Internet

Microsoft has general policy rules for its employees worldwide on the use of E-mail and the Internet. The rules or guidelines with which employees should comply vary from country to country. Microsoft only authorizes use of the network system, E-mail and the Internet for Microsoft's lawful business purposes. Microsoft's aim in providing these indispensable business resources is to provide effective communication and information exchange. You can obtain more detailed guidelines and additional information from the "Employee Handbook" column on Microsoft's internal network system or from the following guideline summary:

- 1) The dissemination or storage of vulgar or obscene content that is pornographic, slanderous or threatening or disparaging of a third party or that violates public order or good morals or is unlawful is prohibited in all circumstances.
- 2) You may not:
 - intentionally disparage a third party and/or falsely represent yourself online;
 - modify information and transmit such modified information to a third party without indicating the modification (for example, by deleting or removing received items, altering E-mail content, etc.);
 - falsify information and/or falsify the sender of the information; maliciously bypass the E-mail system's user privacy system (for example, by creating a false account); modify the E-mail transmission and delivery system, create a false path or truncate information over the Internet.
 - engage in debate relating to politics, religion or culture when using E-mail and the Internet; use E-mail or the Internet for entertainment, or exceed the scope of Microsoft's lawful commercial and business use when using E-mail and the Internet;
 - violate the laws and regulations of the People's Republic of China concerning the use of computer networks or Internet systems.

Any violation of the above rules will be severely punished by Microsoft.

If you have any questions, please contact your manager or a representative of the legal department.

For more updated and detail information about legal and office guideline, please link the website below to reference. <http://sharepointasia/sites/prcweb/msweb/lca/default.htm>

Employee's Personal Information Processing Policy of Microsoft China

1.Overview

(1) Purpose: The purpose of the formulation of this policy is to clarify the situations of Microsoft (China) Co., Ltd. and its branches, Microsoft Asia Pacific Technology Co., Ltd. and other Microsoft employers in China (hereinafter referred to as "Company") dealing with the Employee's personal information (hereinafter referred to as "personal information" or "personal data"), and regulate Company's behavior in processing Employees' personal information. This policy, together with the Microsoft Global Data Privacy Notice for Employees, External Staff, Candidates and Guests (hereinafter referred to as "Privacy Notice") and other notices provided at the time of data collection, explain what personal data Company collects about Employees, how Company uses this personal data, and the Employee's rights to this personal data.

(2) Scope of application: This policy applies to Employees who have signed employment contract with Microsoft (China) Co., Ltd. and its branches, Microsoft Asia Pacific Technology Co., Ltd., and other Microsoft employers in China, as well as other Employees employed by Microsoft entities who are assigned to work in mainland China. (hereinafter referred to as "Employee")

(3) Processing principle and legal grounds: Employee's privacy is important to Company. Company respects the privacy rights of all Employees and Company is committed to process Employees' personal data in accordance with applicable laws, including but not limited to Personal Information Protection Law of People's Republic of China. Company processes personal data of Employees with a lawful processing basis as provided under applicable China laws.

Special Note: In addition to this policy, Microsoft global has developed principles, policies and statements about privacy protection. Company and Employees need to continue to abide by the relevant principles, policies and statements. For explanations of these principles, please refer to the link: <https://privacy.microsoft.com/en-us>; for Microsoft's privacy policy, please refer to the "Privacy Policy" link:

<https://microsoft.sharepoint.com/sites/mspolicy/SitePages/PolicyProcedure.aspx?policyprocedureid=MSPOLICY-804079558-5>; regarding the Privacy Statement for Employee's personal data, please refer to "Microsoft Global Data Privacy Notice for Employees, External Staff, Candidates and Guests" link: <https://privacy.microsoft.com/en-US/data-privacy-notice>.

Employees may also visit the following internal resource sites, such as the Privacy 101 - Home (sharepoint.com) link: [Privacy - Home \(sharepoint.com\)](#) to learn more about Company's policies and practices about privacy.

Note: This policy does not cover Employee's use of Microsoft consumer products as a consumer, or outside of the employment or assignment with Microsoft. This policy is not intended and shall not be read to create any express or implied promise or contract for any benefit, or for specific treatment in specific situations. Nothing in this policy should be construed to interfere with Microsoft's or Company's ability to process Employee's data for purposes of complying with its legal obligations, or for investigating alleged misconduct or violations of Company's policy or law, subject to compliance with local legal requirements.

2. Personal Data that Company Processes

(This may include data that Employee provides to Company, that Company collects about Employee, or that Company assigns to Employee.)

Company processes personal data about Employee (and Employee's dependents, beneficiaries and other individuals associated with Employee's employment) primarily for managing Company's employment relationship with Employee and Employee's workplace facilities/information systems interactions. As to a former Employee, Company processes personal data about a former Employee primarily for legal compliance reasons, etc.

The personal data Company processes can include, but is not limited to, the following,

Name and contact data. Employee's first and last name, Employee identification number, email address, mailing address, phone number, photo, beneficiary and emergency contact details, and other similar contact data. Additionally, Employee may opt to provide Company with additional contact information such as personal email address and/or cell phone number.

Demographic data. Employee's date of birth and gender as well as more sensitive personal data (also known as special category data) including, but not limited to, information about Employee's health. Company may also ask about Employee's parental status and military status.

Company's reasons for processing this data include,

- (1) Where it is necessary to comply with local requirements and applicable law. For example, Company may use this information to comply with anti-discrimination laws and government reporting obligations;
- (2) To monitor and ensure diversity and equal treatment and opportunity;
- (3) To provide work-related accommodations or adjustments, to provide health and insurance benefits to Employee and to Employee's dependents and to manage absences from work.

Where the processing of this personal data is not required by law, Company will seek Employee's consent to process Employee's data and, in the consent mechanism, Company will explain the purposes for which Employee's data will be used. This will be voluntary, and Employee may decide whether or not to give consent.

National identifiers. Employee's national ID/passport, citizenship status, residency and work permit status, social security number, or other taxpayer/government identification number, information needed for social insurance and housing provident fund contributions.

Employment details. Employee's job title/position, office location, employment contract, offer letter, hire date, termination date, performance history and disciplinary records, training records, leave of absence, sick time, and vacation/holiday records.

Spouse's/partner's and dependents' information. Employee's spouse and dependents' first and last names, dates of birth, and contact details, the household registration information and social relations of family members.

Background information. Employee's academic and professional qualifications, education, CV/Resume, current and former employment status, credit history and criminal records data (utilized for background screening and vetting purposes where permissible and in accordance with applicable law or results of consultation).

Video, voice and image. Company may collect and use Employee's video, voice and image data, subject to the requirements of local law, internal policy, or any requirements from consulting with worker representatives (where applicable).

Financial information. Employee's bank account details, tax information, salary, retirement account information, company allowances and other information necessary to administer payroll, taxes and benefits, using and payment information of corporate credit card, related information of business trip and reimbursement, etc.

Learning and Skills Data. As described in the Learning and Skills Data Addendum.

Feedback and sentiment data. Employee's responses to Employee's listening surveys such as Employee Signals Daily Pulse and any other survey tools used subsequently and feedback collected about managers and co-workers via tools like Manager Feedback and Perspectives.

Workplace, Device, Usage, and Content data. Application data (such as data from Office 365, Teams, or Outlook, or internal business processes) including emails sent and received, calendar entries, to-do items, instant messages, building and information system access, Microsoft devices, system and application usage (including telemetry) when accessing and using Microsoft corporate buildings and assets. Please note, more information about the specific types of data Microsoft may use for product improvement purposes can be found in several resources, including the Microsoft Data Program (MDP) addendum. Company may also collect personal data about Employee from third parties or public sources as needed to support the employment relationship or to engage with Employee concerning job opportunities

at Microsoft. For example, before and during Employee's employment or assignment with Company, Company may collect information from public professional networking sources, such as Employee's LinkedIn profile, for recruitment purposes. Company may also conduct lawful background screenings, to the extent permitted by law, through a third-party vendor for information about Employee's past education, employment, credit and/or criminal history. In the event of a natural disaster or other life/safety emergency, Company may rely on public social media posts or other public sources to account for Employees if otherwise unable to contact them. Additionally, if there is an investigation of an incident involving Employees, Company may obtain information relevant to the incident from external sources including private parties, law enforcement or news sources and public social media posts.

In some limited circumstances, with Employee's consent (where appropriate or required), Company may collect personal data for research purposes or other non-employment related purposes, with Employee's consent.

Sensitive Personal Information. The following non-exhaustive types of personal data that Company collect from Employee, as necessary, may be considered Sensitive personal information under applicable Chinese laws, Demographic and biometric data, including employees' health information; and Financial information.

3. Why Company Processes Personal Data

Company collects Employee's personal data for the purposes set out below. Failure to provide Employee's personal data when requested may prevent Company from being able to carry out these tasks and/or comply with Company's legal obligations.

(1) To administer Employee's employment contract, offer letter or other commitments Company has made to Employee.

Company collects and uses Employee's personal data primarily for the purposes of managing Company's employment or working relationship with Employee, and to fulfill Company's obligations under Employee's employment contract, related agreement, or applicable Microsoft policies, including on-boarding, payroll, benefits administration, pension and retirement administration, managing vacation and other types of leave, tax reporting, and the like. A few examples include, Employee's employment contract, Employee's offer letter (e.g., so Company can on-board Employee), promotion history and performance reviews (e.g., so Company can manage Company's employment relationship with Employee), and Employee's bank account and salary details (e.g., so Company can pay Employee or provide HR benefits).

(2) Other overriding and legitimate business purposes

Company may also collect and use Employee's personal data when it is necessary for other legitimate purposes, such as general HR administration, maintaining Company's global directory of Employees and external staff, general business management and operations, disclosures for auditing and reporting purposes, measuring Employee sentiment, internal

investigations, management of network and information systems security, business operations, security, life safety and building management, provision and improvement of employee services, physical security and cybersecurity, data protection, for global diversity and inclusion initiatives, to protect the life and safety of Employees and others in connection with the sale, assignment or other transfer of all or part of Company's business. Company also uses business data and other workplace usage, device and content data for organizational and individual analytics and data insight purposes to improve Microsoft business operations, manager ability, and Employee experience. Company may also use special applications and systems that record Employee performance metrics, such as sales related or code databases for business operations purposes as well as for the purposes of reviewing, rewarding and coaching Employees on their performance and for administration and assessment of training. Company may also process Employee's personal data to investigate potential violations of law or violations of Company's internal policies.

(3) Legally required purposes

Company may also use Employee's personal data when it is necessary to comply with laws and regulations, including collecting and disclosing personal data as required by law (e.g., minimum wage, working time, tax, health and safety, anti-discrimination laws, global migration, and data subject rights), under judicial authorization, or to exercise or defend Microsoft's legal rights, or Microsoft processes personal data for purposes of complying with its legal obligations, or for investigating alleged misconduct or violations of Microsoft's policy or law, subject to compliance with local legal requirements.

(4) Other uses of Employee's data (where permissible and in accordance with applicable laws and consultation requirements)

Company may also collect Employee's internal usage data of Microsoft products, services and internal applications and tools, including business data created by employees and external staff, to measure and improve these products; for product improvement purposes human and machine review of such data might be conducted to train AI models and improve machine learning for Microsoft products and services. Where required by law, Company will seek individual's consent for such usage; and where individual's consent is sought, Company will ensure individual's consent is informed, voluntary, and that individual suffers no adverse consequence from any decision to withhold or revoke the consent.

(5) The Company only collects and uses sensitive personal information for the following purposes as described in the "Why Company Processes Personal Data" section. The Company will adopt strict security measures when processing sensitive personal information,

- Comply with requirements and applicable laws;
- Administering employment contract or other commitments the Company made with Employee;
- HR management; and

- General business management and operation.

4.Change of Purpose

Company will use Employee's personal data only for the purposes for which it was collected, unless Company reasonably needs it for another compatible purpose and there is a legal basis for further processing. For example, relying upon our legitimate interest in recruiting candidates for roles at Microsoft, Company may process personal data the individual provided while researching job openings based on individual's consent. However, once an individual applies for and is successful in obtaining a role, Company may process related personal data for the purpose of entering into an employment relationship with individual.

5.How and Why Company Shares Personal Data

Company will only share Employee's personal data with those who have a legitimate business need for it. Whenever Company permits a third party to access Employee's personal data, Company will ensure the personal data is used in a manner consistent with this policy (and any applicable internal data handling guidelines consistent with the sensitivity and classification of personal data). Employee's personal data may be shared with Company's subsidiaries and affiliates and other third parties, including service providers, for the following legitimate purposes,

(1) In order to carry out the purposes of Company's personal data processing as described above (see section titled "Why Company Processes Personal Data");

(2) To enable third parties to provide services on behalf of Microsoft. Third party data recipients include financial investment service providers, insurance providers, pension administrators and other benefits providers, childcare providers, payroll support services, relocation, tax and travel management services, health and safety experts, facility management, legal service providers, and security services;

(3) To comply with Company's legal obligations, regulations, government clearances, or contracts, or to respond to data subject rights, a court order, administrative or judicial process, such as a subpoena, government audit or search warrant. Categories of recipients include counterparties to contracts, judicial and governmental bodies;

(4) In response to lawful requests by public authorities (such as regulatory bodies, law enforcement authorities, and national security organizations);

(5) To seek legal advice from external lawyers and advice from other professionals such as accountants, management consultants, etc.;

(6) As necessary to establish, exercise or defend against potential, threatened or actual litigation;

(7) Where necessary to protect Microsoft, Employee's vital interests, such as safety and security, or the vital interests of other persons;

(8) In connection with the sale, assignment or other transfer of all or part of Company's business (such as to a potential purchaser and its legal/professional advisers); or

(9) Otherwise in accordance with Employee's consent.

Please note that where legal requirements limit the sharing of Employee's personal data, Company will respect such requirements.

6. Use of Cookies and Web Beacons

Site pages may use cookies (small text files placed on Employee's device). Cookies and similar technologies allow Company to store and honor Employee's preferences and settings, enable Employee to sign-in, combat fraud, and analyze how Company's websites and online services are performing.

Company also uses "web beacons" to help deliver cookies and gather usage and performance data. Company's websites may include web beacons, and cookies, or similar technologies from third-party service providers.

Employee has a variety of tools to control the data collected by cookies, web beacons and similar technologies. For example, Employee can use controls in Employee's internet browser to limit how the websites Employee visits are able to use cookies and to withdraw Employee's consent by clearing or blocking cookies.

7. Workplace Security and Monitoring

Company monitors its IT and communications systems through automated tools such as network authentication and wireless connectivity hardware and software, anti-malware software, website filtering and spam filtering software, security software for cloud-based applications, access and transaction logging, and mobile device management solutions. The primary purpose of this monitoring is Company's legitimate interests in protecting its employees, customers, and business partners. For example:

(1) For systems, applications, and network security, including in particular the security of Microsoft's IT systems and assets, and the safety and security of its employees, external staff and other third parties;

(2) For network and device management and support;

(3) For proof of business transactions and recordkeeping;

(4) For the protection of confidential information and company assets;

(5)For investigating wrongful acts or potential violations of company policy; and

(6)For other legitimate business purposes as permitted under applicable law.

Company also monitors Company's offices, and other workplace facilities, through video monitoring such as closed-circuit television ("CCTV") and badge scanning for security purposes, life safety and building management purposes. CCTV is primarily used at office entrance and exit points, elevator lobbies, rooms where there may be valuable equipment, such as server rooms, and in other selected areas with a high risk for theft or with highly sensitive assets. CCTV is not used in private spaces such as restrooms, nursing rooms or locker rooms. Nor is it used to monitor employee workstations for performance reasons.

Any message, files, data, document, facsimile, audio/video, social media post or instant message communications, or any other types of information transmitted to, through or from, received or printed from, or created, stored or recorded on Company's IT and communications systems and assets (included via the use of personal devices accessing corporate IT systems) are presumed to be business-related and may be monitored or accessed by Company in accordance with applicable laws and workplace agreements (such as employment contract), and subject to Microsoft's own policies on access to and uses of such data.

All Employees acknowledge and consent that the Company has the right to access, review, monitor, image, transfer overseas, search or delete any data or applications stored on the Company's IT and communications systems or access, monitor or search workplaces at any time for the purposes of resources management, business operations, information and other security operations, internal investigations, audits and risk management, compliance with the Company's legal obligations or any other lawful purposes.

8.Security of Personal Data

Microsoft is committed to protecting the security of Employee's personal data. Company uses a variety of security technologies and procedures to help protect Employee's personal data from unauthorized access, use, or disclosure. For example, Company stores the personal data Employee provides on limited access computer servers that are located in controlled facilities, and we protect certain highly confidential or sensitive personal data through encryption in transfer and at rest.

9.Cross-Border Transfer of Employee's Personal Data

Microsoft operates globally and to perform contracts and business operations, carry out human resources management, fulfill legal obligations, and other lawful purposes, Company may transfer personal information collected from Employee in China to locations of the Company's affiliated entities outside of China, for example, the U.S. where the headquarter of Microsoft resides. When Employee's personal information is transferred outside of China,

Company will ensure that such transfer will comply with applicable Chinese laws and regulations, and appropriate and necessary measures will be implemented to provide an equivalent level of data protection in accordance with applicable Chinese laws.

10. Company's Retention of Personal Data

Company will store personal data in accordance with applicable laws or regulatory requirements and retain data for as long as necessary to fulfill the purposes for which the personal data was collected, as documented in Company's corporate data retention schedule.

11. Employee's Rights to Personal Data

Company respects Employee's personal rights according to applicable laws and regulations including Personal Information Protection Law of People's Republic of China within personal information processing activities, e.g., Employee may copy, consult, correct, complete and ask for deleting Employee's personal information under lawful circumstances. In specific circumstances, Company may not be able to respond to Employee's request of exercising personal rights due to requirements by laws and administrative regulations or legitimate purpose of processing personal information.

Employee may exercise related rights via AskHR@microsoft.com.

For reasonable requests from Employee, there is no charges in principle. But multiple and repeated requests in a certain period of time may lead to a certain charge of cost born by Employee.

12. Changes to this Policy

It is necessary to alter this policy as Company continues to grow and progress or the regulations and policies related to personal information are adjusted. Company has the right to make corresponding revisions to this policy from time to time in accordance with changes in Chinese laws and changes in Company's internal production or management policies. Company will notify Employee of the changes in the form of intranet announcements or emails, and explain the details of the changes and the implementation date of the new policy. Employee understands and agrees that he/she is also obliged to check Company's related websites at any time to understand the latest policies and comply with them. If Employee has any questions and/or suggestions about the content of the changes, Employee should submit them to Human Resources Department within 15 calendar days after receiving the notification of the changes.

13.Learning and Skills Data Addendum

This addendum applies to Learning and Skills Data that Company processes about Employees for various purposes, subject to compliance with local laws, its own internal policies, third-party terms of use (e.g., where skills data or training is provided by third parties), and applicable third-party contractual requirements.

Learning and Skills Data is information about Employee's professional development activities, such as training and achievements, skills, and related interests. Sources of Learning and Skills Data include information about Employee's,

- Interactions with Microsoft Learning websites, such as Microsoft Learn or LinkedIn Learning, when Employee authenticates with Employee's Microsoft employee account.
- Microsoft Internal trainings, courses or other offerings delivered by Microsoft, that Employee may take to develop job, work, role or career-related skills. These offerings may be optional, encouraged, expected or even required; may be provided live, online or via audio and video recordings; and may be targeted broadly or scoped to Employee's business, role or function. Examples include, Microsoft's Standards of Business Conduct Training, offerings for Microsoft Employees only on LinkedIn Learning, and trainings offered via company-wide, divisional or team learning portals.
- Third-party trainings or courses offered by Microsoft, or linked to Employee's Microsoft employee account, or that Employee chooses to share with Microsoft. Unlike the internal trainings referenced above, these trainings are delivered by third parties, not Microsoft, or are offered through services such as LinkedIn or LinkedIn Learning. These trainings may be provided via external websites, off-site courses, or delivered (even internally) by third-party resources. Like internal trainings, these third-party trainings may be targeted broadly or scoped to Employee's business, role or function and may be available via commercial or consumer-facing websites. Examples include, offerings on LinkedIn Learning, or courses offered by third parties like Dale Carnegie or others.
- Certifications and achievements, such as Microsoft and third-party certifications Employee earns and chooses to share. Some jobs, roles or functions may require specific certifications. Where that is the case, Employee will receive prior notice of such requirements. If certifications are mandatory, Employee may be required to share information about Employee's successful completion of these certifications.
- Skills Employee identifies or that can otherwise be inferred from Employee's learning or professional activities.
- Participation in Microsoft events, such as Ready, Build, and Hackathons.
- Growth interests, such as the experiences or skills Employee indicates that Employee would like to build for Employee's growth and development in Connects or other contexts, or

the content or material Employee explores related to professional development, career planning, skill building, and other learning opportunities.

- Role-based development, such as hands-on or experiential activities Employee does to gain competence in Employee's role.

Microsoft may process various kinds of data from the above sources including (but not limited to),

- Contact Information and Demographic Data, for example, Employee's name, contact information, job title, job level, profession, etc.;
- Attendance, performance, and completion data;
- Feedback about a particular event, course, training or offering;
- Analytics about Employee's interactions with a training or learning website or service;
- Data about Employee's skills that Employee provides or are observed;
- Photos, videos or recordings (video and audio) of the training activity or event.

Microsoft also collects Learning and Skills Data in various contexts. For example, Microsoft collects Learning and Skills Data when Employee,

- Provides it, for example by sharing Employee's professional development goals with Employee's manager in Employee's Connect, joining a Microsoft internal distribution list or group affiliated with a certification or professional skill, or updating Employee's profile by adding badges designating professional achievements;
- Authorizes a third party to provide it, such as when Employee directs an educational or professional organization to share Employee's professional achievements with Microsoft;
- Registers and participates in Microsoft learning activities, such as attending Ready, Build or a hackathon.
- Uses learning services available only to Microsoft employees and/or external staff, such as when Employee views professional development content or interacts with learning modules; and
- Uses learning services authenticated with Employee's Microsoft employee account, such as Microsoft Learn or LinkedIn Learning (subject to applicable terms of use for the hosting website and any contractual obligations Microsoft has undertaken for access to such data).

Microsoft uses Learning and Skills Data for the varied purposes set out below, which may involve automatic processing using machine learning and artificial intelligence applications, such as natural language processing.

(1)To manage Company's employment or working relationship with Employee, including Employee's career development opportunities.

Company processes Learning and Skills Data for the purpose of managing Company's employment or working relationship with Employee, including fulfilling Company's obligations and commitments to Employee . Failure to provide Employee's Learning and Skills Data when requested may prevent Company from being able to carry out these tasks and/or comply with Company's legal obligations. For example, Microsoft uses Learning and Skills Data to:

- Verify whether Employee has completed training activities required in Employee's role or as required by applicable laws;
- Facilitate, at Employee's direction, professional development and career planning;
- Review, reward, and enhance employee performance and career development;
- Identify career and growth opportunities for employees;
- Determine appropriate resources for a particular customer opportunity or support scenario;
- Assess Employee potential for growth;
- Validate whether Employee has attended training paid for or reimbursed by Microsoft; and
- Assist Employee in identifying content or materials that may be aligned with Employee's growth interests.

(2)To provide and improve Company's products and services.

Company processes Learning and Skills Data to provide and improve Company's products and services. For example, when Employee registers for Microsoft training or certification exams, Company uses Employee's Learning and Skills Data to determine if Employee has completed the training and, if appropriate, meets certification bar. Company may,

- Analyze pseudonymized Learning and Skills Data to determine which learning activities are most popular among new Employee or Employee with certain titles;
- Combine Learning and Skills Data with other business intelligence data to identify and evaluate, on an aggregated basis, the effectiveness of learning products and services. For example, Company may query whether certain learning activities increase customer satisfaction levels, improve employee safety, reduce security incidents, or have impact on career development opportunities or Employee performance; or
- Use feedback from learning activities to improve Company's products and services. For example, Company may receive insights about ways to improve Azure when analyzing aggregated results of Azure certification exams or reviewing feedback received after a training event.

(3)Other lawful purposes

Company processes Learning and Skills Data for other lawful purposes, such as when:

- Necessary for Company's legitimate business purposes, such as running Company's business, conducting business intelligence, for auditing and reporting purposes, managing Company's network and information systems security, and providing and improving employee services.
- Company suspects or discovers violations of law or breaches of Company's internal policies.
- Permissible, with Employee's lawfully obtained consent.
- Company considers it necessary for complying with laws and regulations, including collecting and disclosing personal data as required by law (e.g., for minimum wage, working time, tax, health and safety, anti-discrimination laws, global migration and data subject rights), under judicial authorization, or to exercise or defend Microsoft's legal rights.

14. Microsoft Data Program (MDP) Addendum

This addendum applies to the Microsoft Data Program (MDP) and the business-related data processed by MDP for purposes of debugging, testing, developing, and improving new and existing products and services ("MDP Data"). MDP data may be used to train AI and machine learning models. MDP and the terms of this addendum apply to Microsoft Employee only. External staff and candidate data are specifically excluded from the scope of MDP. More information about the specific terms and scope of MDP can be found at the Learn More page of related chapter, refer to link: <https://privacy.microsoft.com/en-US/data-privacy-notice> . Employee may opt-out to limit their participation in the program at any time, without adverse consequence by clicking <http://aka.ms/MDPOptOut> .

MDP is aimed primarily at the processing of data or information that is transmitted, created, exchanged or stored by Microsoft Employee using Microsoft internal systems, software, services, and assets within the scope of Employee's employment. Microsoft will make reasonable efforts to implement controls to exclude non-business-related data from the scope of MDP, where possible. While those controls are intended to limit the scope of MDP to processing Microsoft business-related data (as described further at the Learn More page of related chapter, refer to link: <https://privacy.microsoft.com/en-US/data-privacy-notice>), MDP may incidentally process certain personal content for Employee that is created, stored or transmitted in Microsoft owned or provided systems and resources. When that occurs, Microsoft will continue to make reasonable efforts to refine its controls to better exclude such data in the future. At all times, MDP's processing of data will comply with the stated requirements for MDP, as well Microsoft's internal policies (including the Responsible Use of Technology Policy, link:

<https://microsoft.sharepoint.com/sites/mspolicy/SitePages/PolicyProcedure.aspx?policyprocedureid=MSPolicy-7777>), as well as local law.

Sources of MDP data include, but are not limited to, emails and calendar information in Exchange, files stored in OneDrive for Business, content of meeting recordings, voice collected on work devices, messages in Yammer and Teams, content on SharePoint sites, diagnostic data from work devices, search data, product and services feedback data, and internal line of business applications such as those applications developed to support sales processes (e.g., MSX). These are representative and non-exhaustive examples of the types of Microsoft business-related data from which MDP may process data. Up-to-date information concerning MDP can be found at the Learn More page of related chapter, refer to link:

<https://privacy.microsoft.com/en-US/data-privacy-notice>.

In addition to content-related data from the above sources, Microsoft may also process various additional kinds of data from the above sources in support of MDP including (but not limited to),

- Basic Demographic Data, including, for example, Employee's name and alias, etc.;
- Meta-data associated with the applicable content, such as time and date information, signals related to authorship and modification of data, document and meeting titles, etc.; and
- Telemetry data, such as data related to product and feature usage, associated with the above content types and services, or machine-related data such as software version history, machine type, operating system version, etc.

Microsoft's use of MDP data is premised on Microsoft's legitimate interest in using its own business data for business-related purposes, as that use strongly exceeds Employee's individual interest in the privacy of such business-related data. Microsoft may process certain MDP data based on Employee's consent, to the extent, (1) an individual's privacy interest would exceed Microsoft's interest in the processing; and (2) local law requires Microsoft to obtain consent prior to such processing. Where consent constitutes the primary basis for processing data under MDP, Microsoft will in all cases ensure consent is voluntary and informed and will also ensure Employee suffers no adverse consequence for refusing to give or later revoking such consent, and gain no specific benefit from choosing to participate or contribute data to MDP.

15.How to Contact Us

If Employee has any question related to personal information processing, please contact AskHR@microsoft.com.

V. Microsoft China Human Resources Information

Compensation Philosophy

At Microsoft, we have a longstanding philosophy of pay for performance. We believe in fostering an environment that rewards you for doing your best work to drive business results. Our compensation programs, which are a key component of your Reward Portfolio, are based on following key principles:

- **Distinctiveness with Purpose:** Drive distinctiveness in support of cultural transformation.
- **Differentiation:** Differentiate rewards for employees who create impact through team results (vs. individual heroics). Relentlessly retain those most critical to future growth.
- **Accountability for business and people results:** Create a stronger linkage of rewards to quantitative performance. Increase accountability for culture and organization leadership.
- **Market segmentation:** Segment company rewards budget by competitive need. More discerningly apply resources to future growth areas.

Payroll Information

Pay Cycle

January – December of each calendar year

Pay Day

Last workday of each month. Please be noted that if your onboard date is before the payroll cutoff day of your onboard month, your salary will be paid via your onboard month payroll; If your onboard date is after payroll cutoff day of your onboard month, your salary will be paid via next month payroll.

Payroll Bank Account

Payroll MUST be paid out in RMB, your bank account should be a domestic account to accept RMB and the beneficiary name must be employee himself/herself. Beneficiary name of other is not acceptable.

Online Payslip

Your Online Payslip of the current month shall be available on and after the Pay Day, last workday of the month. Please go to **ADP Employee Self Service (ESS) Portal** at <https://aka.ms/ADP-MyView> to view/print your online payslips. If you are connected to corpnet, you can access the ESS Portal automatically, no separated log on needed. Please kindly note, this site cannot be added to Favorites for security purpose and please use company registered equipment to log on.

Change of Payroll Bank Account

Please go to the **ESS** Portal <https://aka.ms/ADP-MyView> to make the change by yourself.

Payroll Queries

Please read the **Payroll FAQ** on **HR Web**

(<https://microsoft.sharepoint.com/sites/hrw/Pages/MyPayrollCN.aspx>)

Please raise CRM ticket on **Global Payroll Service Portal**

(<https://onefinance.microsoftcrmportals.com/onepayrollhome/>)

Please read the **Global Payroll Service Portal User Guide** on **HR Web**

(<https://microsoft.sharepoint.com/sites/hrw/doclibrary/hrweb/PayBenefits/GlobalPayrollServicesPortalUserGuide.pdf>) carefully then follow the instructions to raise ticket.

Individual Income Tax (IIT)

Withheld by the Company according to the tax area for employee monthly.

Effective from 1 January 2019, the new calculation rule of individual income tax on salary and wage will be applied for resident individuals and non-resident individuals.

Tax Withholding for Resident Individuals

The "Accumulated Withholding Method" shall be applied when the salary and wages are paid to resident individuals, the withhold agent shall declare the full tax for all employees on monthly basis. If any variance between the monthly withholding tax amount and annual tax payable amount, the residents shall complete Annual Individual tax settlement for comprehensive income from 1 March to 30 June of the following year.

1. Monthly salary tax calculation rule

Salary Tax payable = (The accumulated taxable income * Tax Rate - Quick deduction amount) - Total tax paid in previous month of current year

The accumulated taxable income = Accumulated pre-tax income - 5000 * number of the month of the employment for same employer in current year

Accumulated pre-tax income = Accumulated income - Accumulated special deductions - Accumulated additional special educations - Accumulated other deductions

2. Annual bonus tax calculation rule

Annual Bonus Individual Income Tax = Annual Bonus x Tax Rate - Quick Deduction Amount

Tax table for accumulated year today Income

Bracket	Annual Taxable Income (CNY)	Tax Rate (%)	Quick Deduction
1	36,000 or less	3	0
2	In excess of 36,000 to 144,000	10	2,520
3	In excess of 144,000 to 300,000	20	16,920
4	In excess of 300,000 to 420,000	25	31,920
5	In excess of 420,000 to 660,000	30	52,920
6	In excess of 660,000 to 960,000	35	85,920
7	In excess of 960,000	45	181,920

Tax Table for Annual bouns

Bracket	Monthly Taxable incomr(CNY)	Tax Rate(%)	Quick Deduction
1	3000 or less	3	0
2	In excess of 3000 to 12,000	10	210
3	In excess of 12,000 to 25,000	20	1,140
4	In excess of 25,000 to 35,000	25	2,660
5	In excess of 35,000 to 55,000	30	4,410
6	In excess of 55,000 to 80,000	35	7,160
7	In excess of 80,000	45	15,160

Remark:

- 1.The accumulated special deduction refer to Public Housing Fund and Pension
- 2.Additional special deductions refer to Expenditure on Children's Education, Continuing Education, Medical Treatment for Serious Sickness, Interest on Housing Loans, Housing Loan and Supporting the Old Dependents.
- 3.Other deductions refer to Deferral Pension, Tax benefit Commercial Medical Insurance
- 4.For more information, please refer to Tax Bureau website below or call tax hot line 12366 for support
<http://www.chinatax.gov.cn/n810341/n810755/c3960540/content.html>

3. Annual Individual Income Tax Settlement

After the end of each year, a resident individual is required to calculate his/her aggregate income gained and all qualified deductions for the period from January 1 to December 31 of the preceding year, so as to work out the tax amount to be refunded or made up, which shall be the different between the final tax payable amount based on the above calculation and the tax amount withheld in the preceding year, and file with the tax authority and apply for refund or additional payment of taxes. A Resident individual shall complete annual IIT filing if:

1) the tax amount withheld in the preceding year is higher than the tax payable amount and the resident individual intends to apply for tax refund:

- the aggregate income for the preceding year is no more than RMB60,000 and individual income tax has been withheld.
- the withholding rate applicable to the remuneration for labor services, authors' remuneration or royalties gained during the the year is higher than the annual rate applicable to aggregate income.
- when withholding taxes, the applicant fails to in its filing apply for or fails to apoly for full deduction for expenses, special deductions, additional special deductions, and other deductions or donations determined in accordance with the law or fails to apply for any or all tax preferences for aggregate income.

2) the aggregate income for the preceding year is higher than RMB120,000 and an additional tax amount of RMB400 or more shall be paid, including the circumstance where the resident indivudal gains income from two or more sources, thus is subject to a higer combined tax rate, leading to the tax amount withheld less than the tax amount payable.

*Remarks: please note that Annual Individual Income Tax Settlementis required normally when:

- Your work location with Microsoft has changed (e.g., from Beijing to Shanghai) or your employer has changed in the preceding year.
- You joined Microsoft on or after February 1 in the preceding year, and in the same year

-There are other sources of income, etc

4. Any employee who has changed its tax status from a resident individual to a non-resident individual during the preceding year shall complete relevant settlement with the tax authority before 15th Jan.

Tax Withholding for Non-Resident Individuals

When the non-resident individuals receive the salary and wage income, the individual income tax shall be withheld and paid on monthly basis, the taxable income on non-resident's salary income shall be the balance after the deduction of 5,000 CNY from the monthly income.

1.Monthly Salary income tax rule

Pre-tax Salary Income = Actual Monthly Salary + Taxable Bonuses + Taxable Allowances + Non-payable Taxable Amounts + Other Taxable Payments – Other Taxable Deductions

Taxable Salary Income = Pre-tax Salary Income – 5000

Individual Income Tax = Taxable Salary Income x Tax Rate – Quick Deduction Amount

2.Annual bonus tax rule

Non-resident can enjoy Annual bonus beneficial tax rule once a year. Annual income do not need to combine to monthly salary but calculate separately. The tax rate would follow the rate which Annual bonus divided by six in Monthly tax table below.

Annual bonus tax = {(Annual bonus ÷ 6) × tax rate – Quick Deduction} × 6

Bracket	Monthly Taxable Income (CNY)	Tax Rate (%)	Quick Deduction
1	3,000 or less	3	0
2	In excess of 3,000 to 12,000	10	210
3	In excess of 12,000 to 25,000	20	1,410
4	In excess of 25,000 to 35,000	25	2,660
5	In excess of 35,000 to 55,000	30	4,410
6	In excess of 55,000 to 80,000	35	7,160
7	In excess of 80,000	45	15,160

Additional special deduction:

The newly published Individual Income Tax (IIT) law is fully effective starting from January 1st, 2019. Based on the new regulations, Taxpayer can enjoy additional special tax deductions for the types of expenditures. You can find details on China State Administration of Taxation (SAT) website below:

<http://www.chinatax.gov.cn/n810219/n810744/n3752930/index.html>

Except for the Medical Treatment for critical illness, you can either provide the required information in the proper way as outlined below during the year to the employer (MS China entities) to deduct these items from your salary income for Individual Income Tax calculation on your behalf, or you may deduct them and apply for tax refund by yourselves in the Annual Individual Income Tax Settlement process during March 1st to June 30th of the following year.

You should submit your information through the official APP developed by SAT for IIT calculation, deduction and filing purpose. The APP has been available on both iOS and Android

APP Stores, also available for PC version name as 个人所得税.

Company will download the additional special pre-tax deduction data from the Tax bureau system at beginning of each month to catch previous month application. Since accumulative withholding IIT calculation method is adopted, if you submit additional special pre-tax deduction request or update the request in Tax APP before or within Nov closing, accumulative additional special pre-tax deduction for the year will be captured and deducted in payroll tax calculation.

For new hire or transfer employee, application in the APP can only finish after Microsoft filing your tax with local tax bureau which enable you to select Microsoft as tax withholder in APP. If can't catch year end, employee can get it fix during Annual Individual income Tax Settlement with tax bureau.

For more information, please study SAT website or contact Tax hot line of 12366.

Other Information

Personal identification document number (including but not limited to Chinese ID card, Hongkong, Macau & Taiwan pass, foreign passport, Chinese military card and Foreign Permanent Residence Card), nationality and mobile phone number within the PRC are important information, and they are also important for your benefits, individual income tax filing, and etc. If you have had your identification document renewed, please do notify the AskHR@microsoft.com about the change with providing a scan copy of your updated identification document. If you are not able to notify the company of aforementioned updates, any consequence caused will be borne by the individual.

Stock Award and Employee Stock Purchase Plan

Stock related programs shall be under China SAFE requirements. Company submits SAFE filings for you on regular basis. You have tax liability for your stock earned from the stock related programs according to China individual income tax regulations. Partial of your stock shares is sold for tax withholding upon stock vesting and company helps you to pay it to local tax bureau. Any balance between withholding and actual tax is refunded to you or deducted from your payroll on regular basis.

Your personal identification information (including but not limited to Chinese ID card, Hongkong, Macau & Taiwan pass, foreign passport and Foreign Permanent Residence Card), and bank account information is very important for SAFE filing, tax withholding, stock purchasing and selling, bank remittance. Especially if you're holding non-PRC passport or overseas permanent residence card, or have identification changed or renewed, please do notify the AskHR@microsoft.com by providing a copy of your updated identification document in time. If you fail to do so, any consequence caused will be borne by the individual.

- **Stock Award**

You may view <https://aka.ms/stock> for stock award related information or email to stock@microsoft.com for help.

For detailed stock operation manual and related Q&A, you can visit:
<https://microsoft.sharepoint.com/sites/hrw/Pages/stockhome.aspx>

Morgan Stanley Smith Barne website and hotline can be found from:
<https://microsoft.sharepoint.com/sites/hrw/Pages/gainingaccess.aspx>

- **Employee Stock Purchase Plan (ESPP)**

Learn more information, please visit:
<https://microsoft.sharepoint.com/sites/HRw/Pages/espphome.aspx>

For China SAFE special requirements, please go through:
<https://microsoft.sharepoint.com/sites/hrw/Pages/ESPPparticipanteligibilityCN.aspx>

Fidelity NetBenefits website and hotline can be found from:
<https://microsoft.sharepoint.com/sites/hrw/Pages/gainingaccess.aspx>

* Kindly be noted that if you're leaving Microsoft from Microsoft China, you are no longer allowed to hold any company stock earned according to China SAFE regulations. You will be asked to sell all of your Microsoft stock shares within the required period upon the termination of your employment with Microsoft China. For more detailed information, you can refer to the offboarding check out guidance.

Social Benefits and Employee Benefits

Below please find brief introduction about social insurance, housing fund and employee benefits provided by the Company to employees.

1. Social Insurance

The Company contrubites social insurance for the employees according to the government related regulations.

2. Housing Fund

The Company, in accordance with the laws and regulations of the state and local governments, provides a housing fund and make the corresponding contribution for Chinese national employees.

3. Commercial Insurance and Company Supplementary Insurance

Besides the government required soccial insurance, the Company provides the supplimentary commercial insruances for employees. You can refer to the below details of the coverage and the exact terms described in the insurance contacts. The premium is paid by the Company and the employees need to pay individual income tax according to local tax regulations.

- Life insurance, AD&D Insurance and Dread Disease Insurance
- Medical insurance
The Company also purchases medical insurance for the eligible employees' children and spouse of employee upon enrolment completed by the employees.

- **Maternity insurance**
The Company also purchases medical insurance for the spouse of employee upon enrolment completed by the employee.
- **Worldwide Emergency Assistance (WEA)**
In addition, the Company also established Worldwide Emergency Assistance (WEA) Program for its employees so that employees on overseas business trips can obtain the relevant assistance.

For details, please refer to the Employee Benefits Handbook prepared by insurance company.

For detailed information, please refer to the insurance handbook or visit HRWeb:

<https://microsoft.sharepoint.com/sites/hrw/Pages/lifeadd.aspx>

<https://microsoft.sharepoint.com/sites/hrw/Pages/MedicalandWellnessHome.aspx#>

4. Gifts for Marriage, Childbirth, Hospitalization & Death of Relevant

The Company offers subsidies to employees for the personal event of marriage, baby born, hospitalization or the death of employee's immediate family member. Employees can purchase goods or a gift according to their individual need within the above scope, and then claim it for expenses.

Details can be found on the HRWeb:

<https://microsoft.sharepoint.com/sites/hrw/Pages/Gifts.aspx>

5. Trade union benefits

In accordance with relevant laws of the state and the regulations of superior trade union, the company trade union aims at providing various forms of benefits for trade union members.

1) Fitness benefits for Union Members

Company trade union offers financial assistance to union members for fitness programs. The claim amount for each member is capped at RMB150 per month. Two types of fitness programs are available for members to choose, designated health program or individual fitness expense claim. The open time of selection and fitness activity expense claim will be sent by email from trade union. The submitted receipts must be incurred during the member's active employment with the company; the date on the receipts should be before the deadline of reimbursement in the current calendar year. All receipts of fitness should be issued under the name of 微软（中国）有限公司工会委员会。This benefit can only be used on fitness activities and cannot be used for purchasing outfits, or equipment and so on. New employees' fitness benefit starts from their joining month in Microsoft (China) Co., Ltd. and calculated by month.

More information can be found in:

<https://aka.ms/TUExpense-system>

2) Training and Education benefits for Union Members

Company trade union offers financial assistance to union members to training and education programs. The claim amount for each member is capped at RMB275 per month. Two types of training programs are available for members to choose, designated training program or individual training expense claim. The open time of selection and training activity expense claim will be sent by email from trade union. Invoice title MUST be “微软（中国）有限公司工会委员会”. the date on the receipts should be before the deadline of reimbursement in the current calendar year. The training and education items are mainly related to the employees' own vocational training. New employees' Training benefit starts from their joining month in Microsoft (China)

Co., Ltd. and caculated by month.
More information can be found in:
<https://aka.ms/TUExpense-system>

3) Other union benefits

Besides the benefits above, every member is entitled to additional union benefits of hoildays and events. Please pay attention to your e-mail box since Trade Union would send notice in it.

Please be kindly noted that in consideration of the property of union funds, the company union would adjust the union benefits programs according to relevant laws of the state and the regulations of superior unions. Therefore, specific union benefits programs and implementation details may be adjusted every year. The company union would notify union members of any changes timely. The execution of union benefits program would be based on the latest notice issued by the company union.

6. Microsoft CARES

The Employee Assistance Program (EAP) provides the employees and their family members with access to a full range of services to assist their dealing with a variety of work and non-work related challenges. The EAP services include career development advice, marriage and family counseling, relocation & cultural assimilation, mental healthcare, and legal & financial advisory support.

For the details, you can visit:

<https://microsoft.sharepoint.com/sites/HRweb/SitePages/hrpolicy306.aspx>

Find the contact from below page:

<https://microsoft.sharepoint.com/sites/HRweb/SitePages/SpringHealthGlobalPartners.aspx>

7. Tuition Assistance Program

The Tuition Assistance Program (TAP) offers financial assistance to eligible Microsoft employees for business related tuition expenses. The maximum amount of reimbursement is RMB 20,000 per year. Unused funds will be forfeited and cannot be carried over to following years. Employees should be a full time regular local employee or local hired foreigner with minimum 1 year of service. The last performance review shall not be Zero and the employee shall not receive Zero during the whole program study. In general, it should not conflict with normal work duties.

Tuition programs should be conducted by accredited institutions which are officially endorsed by government associations of schools and colleges. The tuition program should be related to work at Microsoft and be degree education only. Degree study can be bachelor, master or PHD program. Non-degree education and training courses, i.e., education and training without degree granted upon completion, are not eligible for TAP support. All scores shall be no less than 60 (full score 100), or a certificate of successful completion shall be required if the course does not assign a score.

Employee should submit application to enrol the TAP benefit firstly. After full approvals obtained, the reimbursement can be claimed within the notified period according to the notification in Decemember or the following Januaruy.

Please visit the below page for the detailed policy and application process:

<https://microsoft.sharepoint.com/sites/hrw/Pages/tuitionassisthome.aspx>

8. Vacation

Weekend

Employees may take rest on Saturday and Sunday.

Public Holiday

- New Year (January 1st), 1 day holiday;
- Spring Festival (lunar January 1st, 2nd and 3rd), 3 days' holiday.
- Tomb-sweeping Day, 1 day holiday;
- Labor Day (May 1st), 1 day holiday;
- Dragon Boat Festival (lunar May 5th), 1 day holiday;
- Mid-Autumn Day (Lunar August 15th), 1 day holiday;
- National Day (October 1st, 2nd and 3rd), 3 days' holiday;
- Women's Day (March 8th), female employees may take a half-day holiday;
- Youth Day (May 4th), employees who are under 28 will be entitled for half-day leave.

The Company will follow local government regulation for traditional holidays of national minorities.

If public holidays fall on weekends, no in lieu holiday will be offered for Women's Day, Youth Day and national minorities' traditional holidays.

Annual Leave

Below content is the brief of the policy, please visit HRWeb to learn more details:
<https://microsoft.sharepoint.com/sites/hrweb/sitepages/hrpolicy302.aspx>

All vacation requests shall be submitted and reviewed in [MS Vacation](#) system in time.

The policy covers both annual leave and Seniority Days, and the annual leave consists of Statutory Days and Supplementary Days.

- The annual leave that each employee is entitled to is the sum of the Statutory Days and the Supplementary Days. At the beginning of each calendar year, each employee is entitled to 15 days of annual leave.

The Statutory Days are granted according to the length of an employee's accumulated service years for the Company and previous employers. For the purposes of this Policy, such accumulated service years are referred to as Career Service Years, which serves as the basis for determining each employee's statutory annual leave days. For the purposes of simplifying calculation, the Company defines Career Service Year as an employee's age minus 22 years, assuming that every employee starts to work at age 22. If an employee provides satisfactory evidence proving that he or she started working earlier than age 22, the Statutory Days entitled to him/her may be adjusted by the HR.

For employees who are newly hired or whose labor relationship is terminated during a given calendar year, the number of their annual leave days will be prorated based on their actual service days in the year.

The numbers of annual leave days (including Statutory Days and Supplementary Days) entitled to employees with different career service years are as follows:

Career Service Year	Statutory Days	Supplementary Days	Total Annual Leave Days
Less than 1 year	0	Prorated	Prorated
1-10 years	5	10	15
10-20 years	10	5	15
20 years and longer	15	0	15

- Seniority Days: for employees who have served the Company for 5 full years or more, 1 Seniority Day will be granted for each additional year that the employee serves with the Company (capped at 5 days).

Each employee is encouraged to proactively plan and take annual leave and Seniority Days to ensure work/life balance, and is required to observe the due application and approval processes. The employee should work with his/her reporting manager, who shall consider both business priorities and the employee's personal needs, to plan the leave and arrange the work during the leave. If the application is denied by the manager, the employee may still apply for annual leave in the rest of the year.

The Company will arrange the employees' annual leave and Seniority Days according to the specific business needs by giving prior consideration to the willingness and personal arrangement of the employees. Both unused annual leave days and Seniority Days in a given year can be carried over to the next calendar year.

Annual leave and Seniority Days application should be taken in the following sequences:

1. first: Statutory Days carried over from last year
2. second: Supplementary Days and Seniority Days carried forward from last year
3. third: Statutory Days of the current year; and
4. fourth: Supplementary Days and Seniority Days of the current year.

Family Leave

Below content is the brief of the policy, please visit HRWeb to learn more details: <https://microsoft.sharepoint.com/sites/HRweb/SitePages/hrpolicy303.aspx>

Except for lactation leave, all family leave requests shall be submitted and reviewed in in [MS Vacation](#) system in time. Any supporting document required according to the policy should be provided to the MS Vacation designated address.

Employees are entitled to 100% of base pay during family leaves. Unless otherwise mandatorily required by relevant laws and regulations, the payment actually received by an employee from all sources, including social insurance payments, shall not exceed 100% of his/her base pay. For example, if the maternity allowance the employee applies and receives from social insurance

authorities is lower than the base pay, the Company will pay the gap. If the Company overpays the maternity payment during the leave period, the employee shall need to return the overpaid portion to the Company.

Employee who applies for 4 continuous calendar weeks of leave or above at one time will not be eligible for meal benefit.

There will be no compensation for any unused family leaves.

- **Maternity Leave**

- 1) Female employees will be granted twenty (20) weeks maternity leave for child delivery provided that the birth date of the child is during Microsoft employment period.
- 2) Maternity leave may be taken continuously for the full twenty (20) weeks, or at the choice of the employee, be split into two separate parts by taking eighteen (18) weeks continuously at one time, then taking the remaining two (2) weeks continuously at any time during the first 12 months after birth.
- 3) If the term of maternity leave (including all birth related leave days, e.g. leave days for difficult birth, multiple births, maternity rewarding leave, etc.) required by local government where the employee's labor contract is performed is longer than that described herein, such more favorable local regulations should prevail. In such case, the employee may choose to take the leave at one time, or choose to take eighteen (18) weeks continuously at one time, and the remaining days continuously at any time during the first 12 months after birth.
- 4) Maternity leave (or first segment of maternity leave if the employee chooses to split the leave) may start 15 days prior to expected birth of the child but not later than the actual birth date.

Supporting documents required:

- ① Expected delivery certificate, which shows the expected delivery date issued by a certificated medical institution with its chop. Or,
- ② Baby birth certificate.

** About maternity allowance:*

Company will not stop payroll or deduct maternity allowance during the maternity leave period in order to help you to maintain a stable income. That is to say, company pays the maternity allowance to you on behalf of the local government in advance. Therefore, after the end of the maternity leave, you should promptly take the initiative to provide your maternity allowance application or confirmation letter in a timely manner. Company will support you further in the following circumstances:

a. If the government remits your maternity allowance to company account, the tax exemption will be processed in the following payrolls. If the actual maternity allowance is higher than the prepaid amount, the balance will be remitted to you via payroll.

b. If the government remits your maternity allowance directly to your personal account, you should return the corresponding prepaid amount to the company. If the local maternity allowance is higher than the prepaid amount, the balance will be paid via payroll.

- **Miscarriage Leave**

Female employees who underwent abortion or miscarriage are entitled to miscarriage leave, the days of which differ depending on the pregnancy stage when abortion or miscarriage happens:

Pregnancy Stage	Leave Days Grant
Shorter than 4 months	15 days
Longer than 4 months (incl.)	42 days

Supporting documents required:

Miscarriage diagnosis (sick leave) certificate, which shows the pregnant months or suggested off-work period, issued by a certificated medical institution with its chop.

- **Lactation Time:**

For the first six (6) months following the delivery, female employees are eligible for two (2) hours of lactation time per day, or 30 hours of flexible working time per week. For the second six (6) months following the delivery, female employees are eligible for one (1) hour of lactation time per day. Lactation time may be used on daily basis, or taken at one time within one week.

- **Paternity Leave**

- 1) Employees are granted six (6) weeks paternity leave when an employee's spouse gives birth to their child and the birth date of the child is during Microsoft employment period.
- 2) Paternity Leave may be taken continuously for the full six (6) weeks, at the discretion of the employee, be split into two separate parts within 12 months after the child's born.
- 3) Paternity leave starts on or after the birth of the child. All leave time, whether taken continuously or split must be completed within the first 12 months following the birth date or it will be forfeited.

Supporting documents required: Baby birth certificate

** If local government paid maternity allowance for the paternity leave, the same process follows according to the maternity allowance for the maternity leave.*

- **Adoption Leave**

- 1) An employee who adopts a child under 16 during the employee's Microsoft employment period, is entitled to six (6) weeks of adoption leave during the first 12 months after adoption.
- 2) Adoption Leave may be taken continuously for the full six (6) weeks, or at the discretion of the employee, be split into two separate parts within 12 months after the adoption.
- 3) Adoption leave starts on or after adoption of the child, and whether taken continuously or split, must be used within the first 12 months following the date of adoption or it will be forfeited.

Supporting documents required:

Adoption certificate issued by a government authority in charge of the adoption registration having proper jurisdiction over the adoption relationship, which shows relationship between the employee and the adopted child, and effective date/certificate issuance date.

- **Marriage Leave**

- 1) Employees are granted ten (10) days marriage leave when the marriage registration date is during employment period.

- 2) Marriage leave starts on or after the marriage registration date, and shall be taken continuously at one time within 12 months or it will be forfeited.

Supporting documents required:

Marriage certificate issued by a government authority in charge of the marriage registration having proper jurisdiction over the marriage relationship.

- **Family Caregiver Leave**

- 1) Family Caregiver leave supports employees who need time away to care for an immediate family member with a serious health conditions that require significant medical care or treatment.
- 2) Employees are granted maximum of four (4) calendar weeks' family caregiver leave per calendar year regardless of the number of relatives the employee is caring for.
- 3) In the context of this policy, "Immediate family member" includes a spouse, child, son-in-law, daughter-in-law, parent, parent-in-law, sibling, grandparent or grandchild of the employee.
- 4) Family caregiver leave may be taken continuously for the full four (4) weeks, or be taken incrementally. If an employee takes the leave incrementally by working day, the accumulated leave shall not exceed twenty (20) working days within a calendar year. The minimum leave length applied shall be one working day.
- 5) Where spouses are both Microsoft employees then they are each eligible for family caregiver leave. However, they will not be expected to take leave simultaneously unless the condition specifically requires two carers or there are two separate care needs.

Supporting documents required:

Family Caregiver Leave Self-Declaration Form

<https://microsoft.sharepoint.com/sites/hrw/doclibrary/hrweb/country/cn/FamilyCaregiverLeaveSelf-DeclarationFormCN.docx>

- **Bereavement Leave**

- 1) Employees are granted ten work/business days in the event of a death of an immediate family member.
- 2) Employees are granted five work/business days for the death of all other close relatives.

*Immediate family member broadly includes employee's spouse, partner, child, son-in-law, daughter-in-law, parent, parent-in-law, step-parents, sibling, grandparent or grandchild of the employee.

*All other close relatives include employee's cousin, sister-in-law, brother-in-law, aunt, uncle, etc.

- 3) Bereavement leave starts on or after the date of the family member's passing away. Employees do not have to take bereavement leave continuously, however the leave should be taken within 60 days from the family member's passing away, otherwise the un-taken days will be forfeited.

- **Local Government Parental Leave**

The relevant parental leave issued by local governments in accordance with the adjustment of the family policy is applicable to employees in the local city where the labor contract is performed. If the employee meets the requirements of the local government for parental

leave, the employee may apply for parental leave in accordance with the rules of the local government.

<https://microsoft.sharepoint.com/sites/HRweb/SitePages/AboutVacationLeaveTimeOff.aspx>

Sick Leave and Medical Treatment

Below content is the brief of the policy, please visit HRWeb to learn more details:

<https://microsoft.sharepoint.com/sites/HRweb/SitePages/hrpolicy304.aspx>

All sick leave requests shall be submitted and reviewed in in [MS Vacation](#) system in time. Any supporting document required according to the policy should be provided to the MS Vacation designated address.

Sick leave includes Holistic Health Time Off and Full-pay sick leave, and Partial-pay sick leave.

- **Holistic Health Time Off and Full-pay sick leave**

Employees, including new employees in their first year of employment, are entitled to 15 working days of Holistic Health Time Off and full-pay sick leave in each calendar year, 10 working days of which are Holistic Health Time Off and 5 working days of which are full-pay sick leave. For the avoidance of doubt, 10 working days of Holistic Health Time Off are excluded from Medical Treatment Period(except for employee who provides sick leave certificates when applies for Holistic Health Time Off), 5 working days of full-pay sick leave are covered by the Medical Treatment Period.

5 working days of full-pay sick leave can only be used for employee's own illness and medical treatment. Conditions of Holistic Health Time Off please refer to Holistic Health Time Off policy.

Unused Holistic Health Time Off days and full-pay sick leave days cannot be carried forward to the next calendar year and cannot be monetarily compensated.

- **Partial-pay sick leave**

Employees, if having used up the fifteen (15) working days of Holistic Health Time Off and full-pay sick leave within current calendar year, are still entitled to partial-pay sick leave. For the avoidance of doubt, partial-pay sick leave days are covered by the Medical Treatment Period.

If an employee is in one of below situations, the current year's annual leave benefit shall be forfeited. Seniority day will still be valid. If employee has already taken part or all of the current year annual leave prior to the described sick leave, the annual leave benefit in the next calendar year will be forfeited.

- 1) If the employee's Career Service Year is less than ten (10) years, and the taken sick leave accumulates for longer than two (2) months;
- 2) If the employee's Career Service Year is equal or longer than ten (10) years and less than twenty (20) years, and the taken sick leave accumulates for longer than three (3) months;
- 3) If the employee's Career Service Year is equal or longer than twenty (20) years, the taken sick leave accumulates for longer than 4 months.

- **Supporting documents required:**

Except 10 working days of Holistic Health Time Off, the employee, when applying for consecutive sick leave equal or longer than two (2) days, needs to provide diagnosis (sick leave) certificates

and medical records issued by a qualified medical institution, which certificates should specify the issuance date, disease diagnosis and suggested sick leave period, with a doctor's signature and the medical institution's chop affixed on. The sick leave that the employee applies via the system should not be longer than the period suggested by the doctor in the diagnosis (sick leave) certificate (both working days and non-working days will be calculated). If necessary, the employee should further provide the qualification materials of the medical institutions. For sick leave less than two (2) days, the Company has the sole discretion to request the employee to submit sick leave certificates for verification.

Diagnosis (Sick leave) certificates should be submitted to HR within one (1) week after the start day of sick leave through:

- Uploading the scan copy or picture to MS Vacation designated address.
- being sent to AskHR@microsoft.com via email, if the employee could not access to system due to special reasons.
- The Company has the sole discretion to request the employees to submit the original copy of the sick leave certificates. After receiving company's request, the employee should submit the original certificates to HR within three (3) working days.

Application requirements:

- 1) An employee shall apply for sick leave through the company online system (MS Vacation) before the proposed start date of sick leave. If supporting document(s) required, please follow the process to provide accordingly.
- 2) In the case of emergency, the employee or his/her family member shall notify the reporting manager via telephone or other effective communication method on the start date of the leave, report the absence reason and the estimated absence period. The employee should keep his/her reporting manager timely informed about the treatment status and confirm the date when he/she can resume work. And within one (1) week after the start day of the sick leave, the employee should submit a formal application for sick leave through MS Vacation and if supporting document(s) required, please follow the process to provide accordingly. If an employee, for special reasons, cannot apply for leave via MS Vacation, the employee should, within a week following start of the leave, send to HR department (AskHR@microsoft.com) a notice with sick leave certificates (if required) and his/her reporting manager's approval attached; HR will, after having validated such sick leave certificates provided by the employee and the approval of his/her reporting manager, submit on the employee's behalf the leave application via MS Vacation.
- 3) During the Medical Treatment Period, if the employee needs to take leave beyond the sick leave days stated in the diagnosis (sick leave) certificate, he/she shall provide extended diagnosis (sick leave) certificate issued by the hospital prior to the expiry date of the current one.
- 4) If there is any concern over the validity of diagnosis (sick leave) certificates and supporting medical documents, the Company has the sole discretion to request the employee to do medical check-up in any designated hospital, and/or to investigate in relevant medical institution for information accuracy.
- 5) If an employee fails to submit the authentic and valid diagnosis (sick leave) certificate within the prescribed timeline, or submits fake, forged, or otherwise non-authentic diagnosis (sick leave) certificate, the Company has the right to deem any taken leave as absenteeism. Any base pay paid by Microsoft during such absenteeism will be deducted from the employee's monthly payroll.

If an employee takes sick leave for longer than three (3) months, the employee shall, within one week prior to expiry date of the leave, contact his/her reporting manager to confirm his/her

return of work, so that the reporting manager can make arrangement accordingly. Furthermore, the employee needs to provide the post-treatment certificates or health-for-work certificates to his/her reporting manager to determine whether he/she can resume work. The Company has the sole discretion to request the employee to do health check-up in any designated medical institution and assess his/her labor ability in any organization designated by the government. The Employee should cooperate accordingly.

Where upon expiration of the Medical Treatment Period, the employee is unrecoverable according to medical certificates issued by medical institution, or has become totally/ partially disable for work as assessed by any organization designated by the government, the Company will take follow up actions in accordance with applicable national and local labor laws and regulations where the labor contract is performed.

Volunteering Days

Below content is the brief of the policy, please visit HRWeb to learn more details:
<https://microsoft.sharepoint.com/sites/hrweb/sitepages/volunteeringdayscn.aspx>

All Volunteering Leave requests shall be submitted and reviewed in in [MS Vacation](#) system in time.

1. Every employee is granted three (3) working days of volunteering leave each calendar year from 1st day of employment. The minimum application unit of volunteering days is half (0.5) day.
2. Volunteering activities should be public welfare activities organized by Microsoft, government or nonprofit NGO (nongovernmental organizations), not by individual or unofficial organizations.
3. Employee shall take leave after manager's approval.

Personal Leave Of Absence (PL)

Below content is the brief of the policy, please visit HRWeb to learn more details:
<https://microsoft.sharepoint.com/sites/HRweb/SitePages/hrpolicy305.aspx>

Please download Personal Leave Acknowledgement, fill all the required information and get all necessary pre-approvals listed in the policy before submitting leave request in MS Vacation:

Length of leave	Required approval				
	Reporting manager and skip level manager	Functional/segment lead	HR manager	HR director	Area VP
≤2 weeks	v		v		
2~12 weeks	v	v	v		
>12 weeks	v	v	v	v	v

After it, submit Personal Leave of Absence leave request in [MS Vacation](#) system and get the manager's approval in MS Vacation as early as possible. Employee shall take leave after request approved on MS Vacation.

- 1) Only the employees who meet all following conditions can apply for personal leave: which includes, at least have two (2) years of service with Microsoft; the performance review not Zero; all other paid time-off options have been exhausted, such

as carried over vacation and the earned annual leave days in current year prior to the start of the personal leave of absence; and the signed Personal Leave Acknowledgement.

- 2) Personal Leaves are typically not granted for more than twelve (12) weeks. And no more than one year for some special situations.
- 3) Requests are considered on a case-by-case basis according to the needs and circumstances of the individual, balanced with Microsoft's business needs. Microsoft retains sole discretion to grant or deny personal leave requests.
- 4) Employee's compensation and benefits will be affected during the leave period.

Supporting documents required: the signed Personal Leave Acknowledgement

(<https://microsoft.sharepoint.com/sites/hrw/doclibrary/HRWeb/Country/CN/PersonalLeaveAcknowledgement-PRC.docx>)

Public Service Leave

The Company will grant paid public service leave to employees who participate in social activities pursuant to the law, which include exercising the right to vote or to run in an election, appearing as a witness in a People's Court, etc. All Public Service Leave requests shall be submitted and reviewed on MS Vacation in time.

9. Retirement and Severance

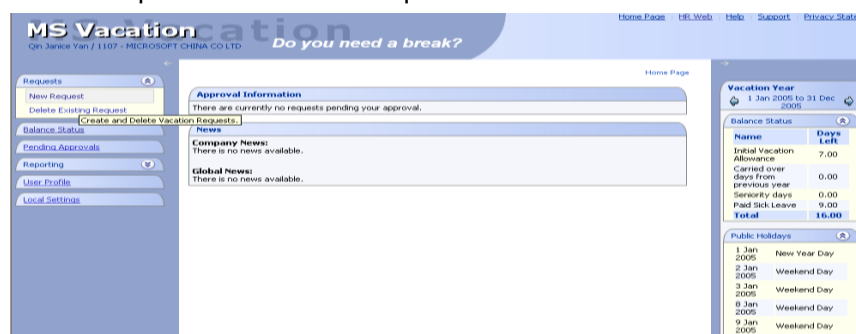
The Company will carry out retirement and severance procedures according to the government regulations for employees that qualify for the retirement and severance conditions specified by the state.

MS Vacation User Guidance

URL: <https://aka.ms/msvacation>, 或 <https://msvacation.microsoft.com>

- How to submit leave request

Click "Requests" -> "New Request".



Select start date and end date of your vacation, Time Zone, select vacation category in the "Request Reason", add your vacation reason in the "Comments".

Click "Add" → Next → Submit to submit your vacation application.

Please be noted that there's no manager approval required for Holistic Health Time Off in MS Vacation. So please do not submit Holistic Health Time Off request together with other leave types.

- How to inquire about vacation balance

Enter into MS Vacation, click "Balance Status" in the menu on the left. Use left/right arrow icon to switch the calendar year. Click "+" before leave group to expand details.

Enter into MS Vacation, click "Reporting" in the menu on the left, and then you may find details.

- How to grant WOB privilege

Enter into MSVACATION, Click "Profile" in the menu on the left to grant work on behalf privilege to others so that they can submit request or approve requests for you.

Name	Days Left
Initial Vacation Allowance	9.50
Carried over from previous year	0.00
Seminar days	0.00
Paid Sick Leave	15.00
Volunteering Days	3.00
OT Conversion	0.00
Total	27.50

How to submit leave supporting document(s)

For those leave types which require supporting document(s), except those which can be uploaded directly in MS Vacation, employee should upload the copies to self-service platform after leave application submitted in MS Vacation.

Step by step process:

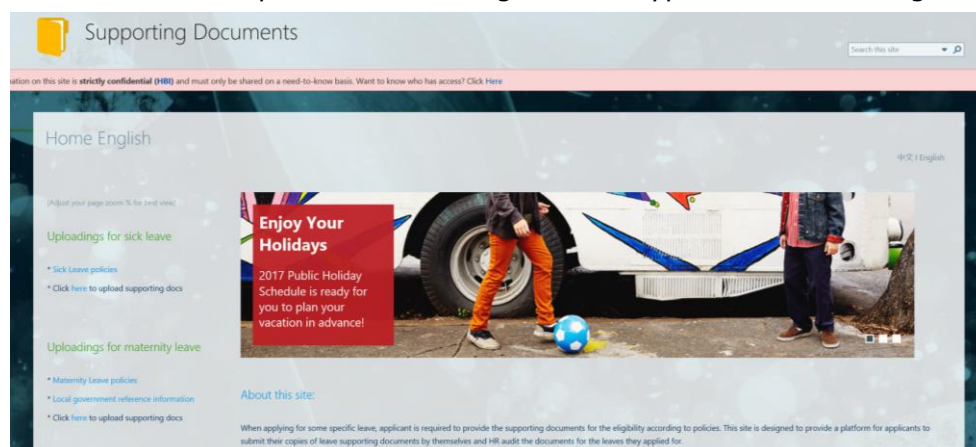
1. Visit self-service platform.



Supporting Documents

<https://microsoft.sharepoint.com/teams/SupportingDocs/>

2. More detailed information related to requirement of supporting documents provided.
3. Select the link provided according to leave type on the left navigation.



4. Fill the table and click "Attach File" to upload the copy of the supporting document(s).




5. If receiving company's request to provide original supporting document(s), employee should submit the original one(s) to HR department within three (3) working days.

Other leave type which required supporting document(s) but MS Vacation self-service

platform currently is not covered, employee should send to AskHR@microsoft.com in time.

How to submit Voluntary Termination Request

Employee can resign from the company by informing the company in writing thirty days in advance

Manager is responsible to submit your voluntary resignation request in Employee Central and upload your resignation letter into the tool.  [Step-by-Step guidance for manager](#).

You also need to submit hard copy of resignation letter with your signature to HR Fesco Desk after triggering the offboarding process

Manage Your Personal Data

Please enter or update your personal data through <http://hrweb/>

It is very important to keep your personal data up-to-date. You may enter / review / update your personal information regularly in HRWeb.

Work / Mobile - People won't find your phone number in Contact Information until you have entered them in HRWeb.

* Mobile inputting format:

	Format	Notes
Mobile	+861398888888	Country code must be specified.

Personal Information Including your legal name, preferred name and differentiator used in Outlook – Please make sure that your legal first name and last name are correctly entered in **HRweb**. Entering your English name or nick name as your legal name is not allowed, it will bring significant inconvenience to you. If you'd like to, you can enter your English name or nick name in "Preferred First Name", you can also enter an "Address Book Differentiator" to differentiate yourself from others who have similar name.

Address Contact Information

Home Address-this information will be provided to your stock broker as your mailing address. Therefore, please make sure it is accurate. If there is any change, please revise it in time.

Cell Phone inputting format:

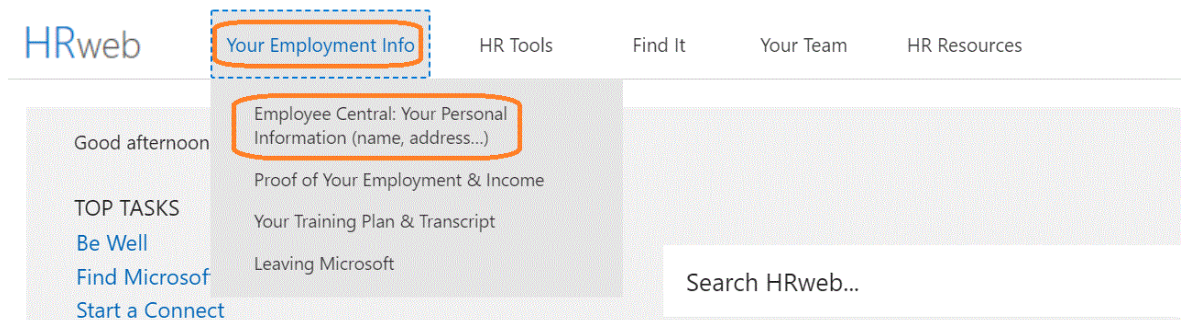
	Format	Notes
Mobile	+8613988888888	Country code must be specified.

Emergency Contact Information

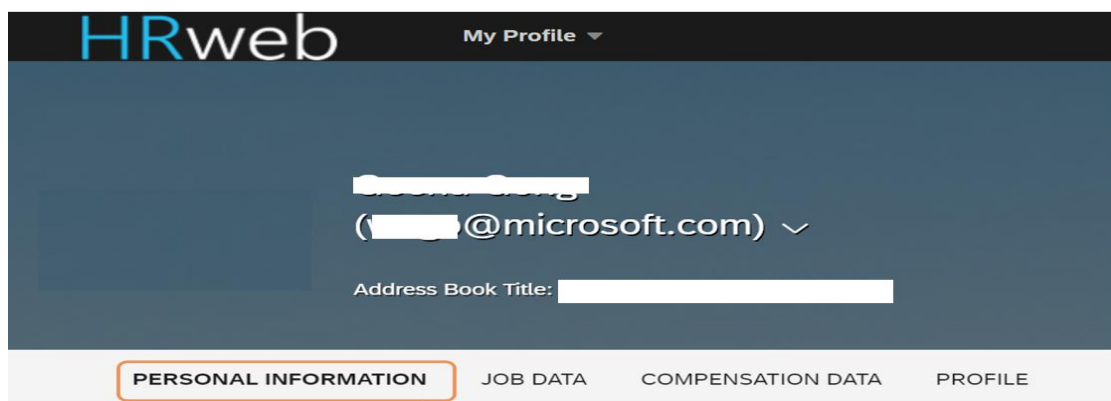
Primary Contact - Emergency contact information is an important information. Please make sure you have it filled in on **HRWeb**. Emergency contact isn't for your manager or company to find you, rather it is to find your relatives or friends in the event of an emergency.

Please follow the instruction below to update personal profile information:

- 1) Open a browser and enter <http://hrweb/>, click "Your Employment Info." and select "Employee Central: Your Personal Information (name, address...)".

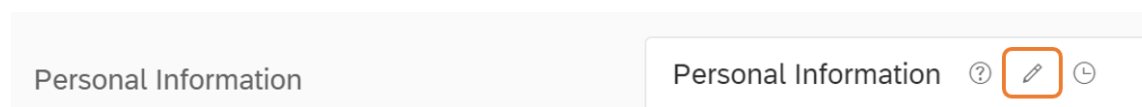


- 2) You will be direct to Employee Central and your name will be automatically shown on following page.



In the page of "Personal Information", please enter/update your **Government ID, Home address, Cell phone, Emergency contact, HuKou, Education** and other **required (*)** personal information.

Click the pencil icon which is located on the right of each tab to update your personal information.



Ex. Please update your "Highest Education Qualification /Degree" and "City of Initial Residence (Hukou)" under "Country Specific Information" of "Personal Information" tab.

Personal Information

Show 8 more fields

Country Specific Information

Country/Region*

China

Highest Education Qualification/Degree*

Do you identify as Transgender?

Gender Identity

Sexual Orientation

Disability Status

Type of Disability

Degree of Disability

Military/Veteran Status


City of Initial Residence (Hukou)

Add Country Specific Information ?

Cancel Save

Under the tab of "Contact Information", you can update your work Mobile number. Click the pencil icon which is located on the left side of "Contact Information" tab, to modify your work phone or click "Add" to add additional contact information.

Contact Information

Contact Information ? 

Business @MICROSOFT.COM ★

Mobile 86 ★

Contact Information

Email Information

Email Type* Email Address* Is Primary*

Business @MICROSOFT.COM Yes

+ Add

Phone Information

Phone Type* Country Code* Telephone Number* Is Primary* GAL Indicator

Mobile 86 Yes No Selection

+ Add

? Cancel Save

- When you finish the editing, please click Save, then the updated information will be submitted in the system and it will take about 24-72 hours to reflect in HRWeb, but will take a bit longer to reflect in other downstream systems.

Performance and Development

Our success as a company depends on continually advancing our strategy and executing quickly, efficiently, and with greater excellence in the way we develop, sell, and support devices and services. Achieving this relies on a One Microsoft culture in which individuals are motivated to do their best work together. Working with others to drive broader results makes this a great place to work. Rewarding employees for their impact to the business reinforces the importance of those results. Giving and receiving feedback, coaching, and engaging employees to learn, grow, and deliver their best work promotes great business contributions and career experiences at Microsoft.

Performance and Development Objectives:

- Drive impact-oriented collaboration and teamwork to achieve greater business results.
- Create mutual accountability for driving team, business, and customer results.
- Reward contributions and business impact.

For more updated and detail information about Performance and Development, please visit the website to reference at [HRweb - Performance and Development Philosophy \(sharepoint.com\)](#).

Connects

Connects provide business-aligned opportunities throughout the year for employee self-reflection, and enrich conversations between employee and manager not only to look back, but also plan forward. Connects focus on short sprints of work: an employee's previous few months of work and the next few months ahead. Connects help employee and manager to understand the impact of the employee on team, business, and customer results and identify opportunities of even greater impact going forward.

Feedback

Feedback is an important part of continuous improvement when delivered in a timely, constructive way. Feedback can be collected by a manager during the year via 1:1 conversations, through email, or through the Feedback tool, which is open all year.

Promotions

Promotions will be based on factors such as business need and employee readiness. For example, when business develops and thereafter a role expands, there could be an opportunity for promotion, meanwhile the employee in position develops required skills or competencies and begins contributing at a higher level, which can be recognized with a promotion.

One-on-One Regular Meetings

The performance and development process is the most effective when managers and employees meet regularly and maintain an ongoing dialogue about progress against objectives and business priorities. Performance and development management is not merely a few isolated events during the year; it is a continuous process that requires both manager and employee engagement.

For more updated and detail information about performance management, please visit the website below to reference

<https://microsoft.sharepoint.com/sites/hrw/pages/performanceanddevelopmenthome.aspx>

Inbound / Work Permit / Residence Permit Assistance for Foreign Passport Holders*

Visa Desk Vendor Contacts

City	Vendor Contact Email
Beijing	Microsoft Visa Desk < msvisa@microsoft.com >
Shanghai	Visa Desk < Immigration@ciicsh.com >
Suzhou	Microsoft Visa Desk < msvisa@microsoft.com >
All Other Cities	Microsoft Visa Desk < msvisa@microsoft.com >

Employee Responsibilities

- Employees must work closely with the visa desk to keep their immigration documents (work/residence permits and registration certificate) valid at all times.
- Employee to sign Attestation/Warranty letter as a confirmation they understand their obligations while employment with Microsoft (China) Co., Ltd.
- To maintain compliance and avoid government penalties, employees must keep their and accompanying family's immigration documents updated and inform the Visa Desk of any actions taken. The immigration documents include the (1) Police Registration Card (Temporary Residence Registration Certificate, TRRC); (2) Work Permit; (3) Residence Permit; and (4) Passport.
- If your nationality has been changed, please inform AskHR@microsoft.com before the new nationality takes effective. So that HR can prepare the employment and relevant documents for the new nationality. Employee should actively provide the updated materials. Any impact and risk caused by the change shall be borne by individual.
- Before leaving Microsoft, employees must provide their original work permit and resident permit for cancellation, as required by law.
- Employees must abide by Chinese laws when in China and must not engage in any illegal activities.

Renewal Application Process

- Visa vendor staff notifies the employees by email of the documents required to process the inbound work/residence permit applications and renewal application. Employees must send an approval email from his/her business manager to initiate the renewal process.
- Visa vendor staff assists the employees with the preparation and review of their applications for work/ residence permits.
- Employees must follow up on required actions, as instructed by the visa vendor staff, to maintain compliance with government rules and regulations.

* Taiwan, Hong Kong and Macao residents no longer required to obtain work permit for employment in Mainland China from August 2018.

Other Information

Reference Check

If you are asked to provide information about exit employees for reference check purpose, please submit your request via [ASK HR](#) (<https://microsoft.sharepoint.com/sites/hrw/DocLibrary/HRConf/Staffing/Recruiting/Tools/ReferenceCheckGuidelines.docx>). HR will provide standard reference check for exit employees

VI. MICROSOFT CHINA EMPLOYEE BUSINESS TRAVEL POLICY and GUIDELINE

Explore MSTravel

Visit <http://aka.ms/mstravel> for all your travel needs:

- Microsoft's Global Travel Policy
- Apply for a Corporate Card
- Travel agency contact details
- Book your travel
- Find training on booking your travel
- Email: mstravel@microsoft.com with questions or for support.

Company Travel Policy & Guidance

Travel Policy

Employees must responsibly utilize Microsoft assets while traveling on Microsoft business. Read both the [Travel Policy](#) and the [Travel Policy Guide](#) before you book travel. [Travel Policy and Travel Policy Guide](#).

Reservations

All air travel, hotel and car rental reservations must be booked through [MSTravel Online](#) or by phone via the [Designated travel Agency](#). Before making your booking read both the [Travel Policy and Travel Policy Guide](#).

Payment

According to [Corporate Card Policy](#), You must obtain and use a Corporate Card to pay for business related expenses. Employees holding an Amex Corporate Card should use the Corporate Credit Card for travel expenses. In the case that the company's credit card cannot be used, a considerable, recordable and traceable means of payment can be used, such as personal credit card. Employees shall keep payment records for future reference or provide payment records as required for reimbursement, and the reason why Corporate Credit Card wasn't used should be noted in the remarks of expense reimbursement. In all cases, cash payments should be avoided as much as possible, and payments in cash should only be made in rare reasonable circumstances where credit cards or electronic payments are not accepted. And this should be specifically noted in the remarks of expense reimbursement.

Note: For expenses lack of clear and accurate supporting documents can't be reimbursed.

Know your itinerary & destination

- Obtain any required business travel visas and ensure you have valid travel documentation before your trip.
- If you travel to [an extreme risk destination](#), you must obtain approval from your manager and VP.
- It is your responsibility to inform the [Regional Security Manager](#).

Airline

- [Approved/Preferred program airlines](#) should be used whenever possible.
- Air travel should be booked with a minimum of **14 days in advance**.
- Use good judgment and choose the lowest reasonable airfare.
- Seats must be booked in **coach/economy class** for every flight segment of 7 hours or less.
- Do not allow your loyalty program choice to drive more expensive reservations

Car

- Employees are expected to consider ground transportation options before renting a car
- MStavel has preferred agreements with **Avis, Sixt and National/Enterprise** that include primary insurance
- The most economical car size, compact to midsize, is reimbursable. A full-size car is reimbursable only when three or more employees are sharing a car or customer transportation is required.
- Visit the [Car rental](#) page to see more information.

Hotel

- Reimbursement for lodging is limited to a standard single room. Room upgrades are not reimbursable.
- MStavel [Preferred hotels](#) should be used where available.
- Review the Microsoft Preferred hotel options including peer reviews at <http://aka.ms/tripism>.

Insurance

The Microsoft [WEA Program](#) provides all Microsoft employees (FTEs) on international business travel with emergency medical, security and travel assistance. Microsoft partners with International SOS, the world's largest medical and security-assistance Company to co-ordinate the program. Information about the WEA program and Non Medical insurance guidelines can be found [here](#).

Escalations

Any service feedback/ escalation should be raised through travel agency as a 1st point of contact. If you need further support please refer to: MStavel@microsoft.com.

China Available information:

1.MS China designated travel agent - CITSGBT

The normal working hour is 09:00-18:00, Monday to Friday.

National Call Center: +86 10 8715 5299

Email: ms.china@citsgbt.com

2.MStavel OBT [Link](#)

To get started access connect.citsgbt.com from your mobile and follow the step-by-step instructions in the [Mobile Connect Lite user guide](#).

Sarch 国旅运通服务号 in Wechat→我的差旅→在线预定



OBT Navigation Support Team at email: systemsupport.cn@citsgbt.com or
Tel: (86) 21-2306-7262.

3. Emergency and After Hour Call Center for travel service

Tel: +86 10 8715 5299

The emergency service fee of CNY 63 will be charged on a per call/case basis.

4. Outbound visa service-China visa desk (CITSGBT)

1) MS Beijing West Campus (on-site desk)

Telephone number: +86 (10) 59165194 (Zhang Bo)

Email: v-bozzha@microsoft.com

Covering area: Beijing West Campus, Chengdu, Shenyang, Wuhan, Xi'an, Chongqing, Qingdao, and Jinan.

2) MS Shanghai Huaxin office (on-site desk)

Telephone number: +8621 61887022

Email: v-cayin@microsoft.com

Covering area: Shanghai, Hangzhou, Nanjing, Suzhou, Wuxi

3) CITSGBT Guangzhou Headquarter (off-site service)

Covering area: Guangzhou, Fuzhou, Shenzhen

Lancy.zhou +8610 87155227

Amanda.wang +8610 87155226

Email: vd.can@citsgbt.com

Address: NO.12th floor, East Tower, Fortune Plaza116, East Ti Yu Road, Guangzhou, China, 510620

Note: Employee must be over 6 months of on-boarding to allow go through Amcham channel for U.S. visa application. (Onboarding time should refer to the labor contract signing time) Or

contact visa deck for social channel interview appointment for length of service of less than 6 months.

5. Corporate Credit Card service support

1) ICBC&AE corporate card

ICBC group hotline(24/7): 4008795588(domestic) ,86 10 95588 (overseas)

VIP service team: vipgroup1@mdk.icbc.com.cn(for feedback,communication,escalation during business hours)

2) CMB&AE corporate card

CMB group hotline(24/7):400-820-5558(domestic), 86 21 68644828 (overseas)

CMB designated account

manager: sahan@cmbchina.com, 18514046661/ baiyue@cmbchina.com; 18301440976 (for feedback,communication,escalation during business hours)

Any questions related to travel program, please contact MSTravel (Alias: mstravel),

Or join in [YAMMER](#) -MSTravel Yammer community to both share and learn with other travelers.

VII. MICROSOFT CHINA EMPLOYEE BUSINESS EXPENSES REIMBURSEMENT

Meal and Entertainment

Employee reimbursement for meals during business trips

Employee meal expenses on business trips are the expenses incurred on business outside the city where the employee lives. The employee may be reimbursed based on the actual receipt and should expense each meal as a separate line item. The standard for reimbursement shall not exceed RMB¥300 per day within China and US\$75 per day for overseas trip (with exceptions approved by GCR CFO or his or her designee). The recommended standard is US\$15 for breakfast, US\$25 for lunch and US\$35 for dinner. No reimbursement will be made for the relevant meal expense if, on an overseas trip to participate in a particular activity, the organizer of the event provides breakfast, lunch or dinner.

Entertainment expenses

Entertainment expenses are expenses incurred during certain business negotiations with clients, suppliers or partners. The employee shall be reimbursed according to the actual receipts.

Please refer to "[PRC Policy on Gift, Entertainment, Travel Sponsorship, and Charitable Donation](#)" for more details:

LEGAL COMPLIANCE POLICIES: [Anti-Corruption](#)

Pre-approval must be obtained *before* any of the following activities takes place:

- a)** Giving a gift to a Government Official or Commercial Customer which, either by itself is worth more than RMB300 or cumulatively with prior gifts to the same Government Official or Commercial Customer during the same fiscal year exceeds RMB 600 in retail value;
- b)** Paying for entertainment for a Government Official or Commercial Customer valued at more than RMB 300 per occasion
- c)** Paying for meals or refreshments for a Government Official or Commercial Customer valued at more than RMB 300 per occasion or RMB 900 per day.
- d)** Paying for overnight lodging or airfare for a Government Official or Commercial Customer, regardless of value.

Meal expenses for meals between employees who work in the same city.

Expense occurs in the one-on-one or one-to-many meeting between the superior manager and employees in the same city, the meal fee involves in the team activity or supervision, it should be categorized as team morale expense.

Late Meals

Valid tax invoice for late meal for work after 7pm AND actual working hours exceeding 8 hours in the working day, or for work in weekends / government public holidays, can be reimbursed if the manager prior approval is obtained. Late meal reimbursement cap: RMB40 per meal.

Employee Personal Vacation

Combining personal vacation with business travel

If personal vacation is combined with business travel, the employee must:

- Incur no additional expenses for the Company; and
- Obtain approval from his/her department manager.

Use of corporate discounts for hotel reservation and automobile rental for personal vacation

During personal vacation employees may use the prices contracted by the Company for hotels and automobile rentals. However, automobiles rented during an employee's personal vacation are not covered under Company insurance.

Telephone Charges

Mobile Fee Claim

Based on current China mobile phone policy, MS China only centrally pays for mobile fee which is under company name. Reimbursement for mobile fee under individual name is no longer supported (Since 01/01/2023). There are exceptions that mobile fee under individual name could get reimbursed through T&E, which apply to employee Individual Income Tax.

- Temporary overseas travel mobile phone expenses under personal name. Please provide the Telecom operator's payment details and invoices, submit through Myexpense / Concur.
- New hire's first two months mobile fee under personal name is still eligible to reimburse from the company.

The company understands your business needs for mobile communication and local mobile phone charge reimbursement practice based on actual spending.

- Reimbursement is capped at RMB1000/month per Sales and Marketing staff if approved by manager
- Reimbursement is capped at RMB400/month per non Sales and Marketing staff if approved by manager

New employee either to use the company provided mobile phone number for business purpose or to transfer your mobile phone number to the company account within 2 months upon on board date. For any inquiries, please contact [Finance Digital Assistant](#) (FDA) for help. For details, please refer to New Employee MP User guideline via the link:

[China Mobile Phone Charge Guideline.](#)

Travel Insurance

Scope of the insurance coverage

When on business trips, employees are covered under the following insurance

- Automobile liability insurance; and
- Formal employees also have travel accident insurance.

Other travel insurance purchased by individual employees

The Company does not reimburse employees for any travel insurance purchased individually.

Loss of Company property

The loss of Company property should be reported immediately to the local insurance agent and to Risk Management, which handles insurance claims worldwide. Indicate in the report the date and the location of the loss of Company property, the type of loss (fire, theft, etc.), and the estimated amount of the loss (if known).

Loss of personal property

Employees are personally responsible for the safekeeping of their personal property during business trips. The Company will not make reimbursement for any lost personal property.

Miscellaneous

Carrying laptop computers

Do not include laptop computers in checked-in luggage. Carry it with you!

Reimbursement Procedure

Expenses for business trips must be accurately recorded on the expense reimbursement form d submitted for reimbursement within 60 calendar days of incurring the expense. The employee submits the expense online and uploads the fapiao image. According to the uploaded image, manager can approve the expense report. The employee needs to print out the cover page and bonds with fapiao. Then drop off the document to the collection mailbox in the office. Big invoice/receipt please directly bind with Cover page, small invoice/receipt please stick on A4 Paper & bind with cover page. [Video example](#) .

After the manager approved the expense and hardcopy received by Dalian Accenture team, the payment would be made. Please attach the official tax receipts when applying for reimbursement. All the receipts (including oil fee and visa fee etc.) must be made out according to below instruction:

Microsoft China Suzhou Branch employee issued fapiao with title "Suzhou Branch of Microsoft (China) Co., Ltd."

MS China head office and other branches employee issued fapiao with title:"Microsoft (China) Co., Ltd."

The detailed fapiao issuing information is as following:

公司名称	公司地址	税号（纳税人识别号）	电话	开户行	开户行账号
微软（中国）有限公司	北京市海淀区丹棱街5号	91110108600040399G	010-59170500	中国银行股份有限公司北京知春路支行	324656010847
微软（中国）有限公司苏州分公司	苏州工业园区星湖街328号创意产业园18号楼	9132059407274739XH	0512-69838592	中国银行股份有限公司苏州工业园区支行	531362850086

Policy on exceeding the prescribed time limit for reimbursement

- A claim should be completed for all expenses within 60 calendar days of their occurrence.

The calculation of 60 days starts from the earliest **expense occurred date** in your expense report, to the last submission date of the approved expense report

- Area GPO is authorized to provide exceptional approval for the expense report to be submitted after 60 days of the expense incurred. Only justification not ascribed to any employee faults may be accepted or else, the submission will be recorded as violation in both local and global dashboard with expense reimbursed upon line manager's approval.

Reimbursable expenses

- Reasonable and necessary to conduct Microsoft business;
- Directly attributable to conducting Microsoft business;
- Compliant with the Microsoft Standards of Business Conduct;
- Properly documented, substantiated, and submitted timely; and
- Approved in accordance with Microsoft Signature Authorization for Expenditures (SAFE).

Non-reimbursable expenses

For Non-reimbursable expenses, you can refer to the below policy link:

- [Employee Expense Reimbursement Policy](#)
- [Employee Expense Reimbursement Procedure](#)
- [GCR Expense Guidance](#)

Example of Non-reimbursable expenses specific for GCR:

- Line and train club memberships
- Expenses incurred and/or submitted on behalf of the expense reimbursement approver
- Expenses incurred by external staffing (vendors, suppliers, agency temporary workers)
- Expenses incurred on behalf of another employee
- Insurance premiums
- Late fees and interest charges due to untimely submission of expense reports
- Personal funds not related to Microsoft business
- Local transportation fee if monthly gas is claimed
- Items should go through PO process for those procurement policy required (PO exception list please check from Procurement policy (https://microsoft.sharepoint.com/sites/ms_policy/Pages/Policy.aspx?policyid=MSPOLICY-2134984086-31)).

Reimbursement of air tickets

- Economy class can be reimbursed
- The business class can be reimbursed only after obtaining **pre-approval** of CVP (Corporate Vice President) or AVP (Area Vice President)
- Do not allow First class reimbursement

Notes of Reimbursement

Specific steps for applying for reimbursement

- **For airfare, flight**

When booking air ticket, MS FTEs need to pay airfare by ICBC/AMEX card. Domestic trip and international trip require attaching AMEX E-invoice with RED Chop from the designated travel agency.

If the airline ticket has been issued but the employee's trip is subsequently cancelled, please contact Microsoft designated travel agency to get the ticket refund, refund will direct deposit to employee's personal bank account; the employee can submit the AMEX E-invoice with RED Chop to reimburse the incurred penalty of return.

- **For rail travel**

When rail tickets are purchased from MS designated travel agency, AMEX E-invoice with RED Chop from the designated travel agency is required for claim purpose.

For tickets bought in the train station, please submit original rail Fapiao for T&E reimbursement.

Employee shall click [Finance Digital Assistant](#) (FDA) to create TKT to contact with AP team and to send back any refund amount obtained from the rail company or the agency after claiming the ticket fare from MS.

- **For lodging**

For VAT receipts issued by hotels, if no details are listed, a separate detailed statement or hotel folio must be obtained from the hotel and submitted together with the receipt. The hotel need the VAT sepecial fapiao.

Airfare, flight – employees should use the “lowest ticket price” offered by Microsoft China’s designated travel agent.

Rail Travel - Rail travel should be made through the designated travel agency or on-line booking tool where available. Where the service is not available or logistics restrict pre-purchase, they may be purchased directly from the rail company/station. Employees should follow the MS business travel guideline to use the “lowest ticket price”. Employee could purchase first/second class train ticket. If an employee need buy business class with reasonable purpose, please ask for manager’s pre-approval.

The reimbursement receipt is the original train ticket, and the refund reimbursement receipt is issued by the railway department (to be collected at railway station). Online booking details & online refund details cannot be used as reimbursement vouchers. Please select the expense category as “Ground Transportation” for reimbursement.

Meals – meal expenses during a business trip out of town.

If out of town on a business trip (for less than one month) you can report RMB¥300 (US\$75) per day.

Work meal expenses cannot be reimbursed because the Company provides employees with meal cards.

The Company does not reimburse meal expenses for meals between employees who work in the same city.

If it is meal for conference, please select the expense category of “Meals/Seminar , training, conf ” for Conferences, Seminars, Intr-Co Mtgs / Trng.

If it is for Morale, please select the expense category of “Employee Morale | Gift & Entertainment” or “Employee Morale | Meal/Drinks” basing on the spend natural.

If it is for entertainment for commercial customers, please select the expense category of "Entertainment -external", And give a brief description about the Full name list, Title & Firm, Business purpose, and place as per the system instruction.

If it is for expense related to government officials, please select the related Government official expense categories according to the expense nature. And give a brief description about the Full name list, Title & Firm, Business purpose, and place as per the system instruction.

Lodging –the room, telephone and laundry expenses

Please claim the meal expenses incurred at the hotel separately from lodging expenses and obtain separate receipts if possible. Enter the room, telephone and laundry expenses under the the expense category of "Hotel - Domestic" or "Hotel - International"; select the expense category of "Meals - Travel" for meal expenses.

Other travel expenses – automobile rental in business travel place-- Ground Transportation, highway tolls- Tolls/Road Charges, fuel costs-Car | Fuel & Maintenance, parking-Parking.

With the manager's approval, upon actual occurrence, reimbursement of fuel cost for privately-owned personal vehicle use for business is capped CNY500 per month applicable to sales and marketing department employees, CNY200 per month for other employees (The provision does not apply for ARD).

If the employee claim fuel cost monthly, he/she may not claim any other fee related to transportation incurred in local (taxi fee to airport or station for business trip is not included).

If the employee drives his/her own personal motor vehicle for business purpose, the total monthly fuel cost claim should cover all the related cost. Other personal motor vehicle cost such as highway tolls, parking fee, designated driving fee can't be reimbursed.

Employee morale – For invigoration the team, or team-building. For example, welcome lunch for the new team member.

The expense report must include the business purpose, place, type of entertainment, and full names of the recipient employees.

Ground Transportation- taxi fee in working city including ride-hailing service fee. Please indicate the start location, the name of the client or the reason (overtime, departmental activity, etc.). For the ride-hailing service, in addition to Fapiao, please also submit travel itinerary (issued by the ride-hailing platform) .

Exchange Rate – The exchange rate has been pre-loaded in the system for all overseas travel expenses to convert into RMB to reimburse.

Employee should fill in the correct foreign currency code in the field of "Currency". For out-of-pocket claims, employee can change the pre-loaded rate to the actual rate and must ensure the accuracy of the rate, then the system will convert the amount into CNY automatically.

Please find the correct currency and reasonable exchange rate in the below link:

<https://msit.powerbi.com/groups/me/dashboards/13cec393-7e2e-4243-a384-e09a9c793294>

Employee shouldn't manually convert the amount in foreign currency to the amount in CNY and fill in the amount in CNY directly.

Entertainment expenses – Meal expenses incurred when inviting guests. Please indicate the name of the guest(s), their position(s) and the name of their company; the number of attendee; the place where they were entertained; the amount of the entertainment expense and the time the expense was incurred; the subject of the business talks. Please refer to "[PRC Policy on Gift, Entertainment, Travel Sponsorship, and Charitable Donation](#)" for more details.

LEGAL COMPLIANCE POLICIES: [Anti-Corruption](#)

Expenses Categories (mainly used):

1. **Supplies - Computer Equipment** — payments for computing supplies (some emergency requirement e.g. mouse, electrical source etc.). Please note: **If the goods can be procured from the vendor that designated by Microsoft, it should be bought from the Vendor by PO process. It cannot be procured personally and reimbursed by T&E.**
2. **Employee Development/Training** — participation in training as required by the department (requires HR confirmation)
3. **Seminar/Course fees** — registration fees for attending meetings, and meals at conference.
4. **Expenses made for or on behalf of Government Officials** — should be claimed under correct Government official expense categories according to the expense nature.

Employee should strictly comply with Anti-Corruption Policy, any failure may result in disciplinary action, up to and including termination.

Please refer to MS Policy for more detail about 'Anti-Corruption policy':

LEGAL COMPLIANCE POLICIES: [Anti-Corruption](#)

For question or concern about the expense in relationship to the Anti-Corruption Policy, please contact Control & Compliance Working Group Alias lca-c@microsoft.com for guidance.

Notes:

Select correct expense category when reporting T&E Expense to avoid a delay in receiving reimbursement.

Check whether the amount claimed is the same as the amount listed in the related tax invoice or overseas receipt.

The handbook only highlights operational key steps for T&E policy, please refer to MS Policy to find the more details.

- [Employee Expense Reimbursement Policy](#)
- [Employee Expense Reimbursement Procedure](#)
- [GCR Expense Guidance](#)

Submit the Expense Report online

For non-Service group employee, please use: aka.ms/MyExpense to filling in the travel expense. The T&E expense claim will be paid in RMB. For detailed process, please contact with Finance Digital Assistant (FDA).

If you are an Service group employee, your T&E expense claim should be filed under Concur (<https://expense.microsoft.com/>).

Account for reimbursement

Please submit your expense account information in SuccessFactors Employee Central (EC) tool before submitting your first application for reimbursement.

Reimbursement may be made in Renminbi to any savings account or credit card in Chinese banks.

***Note:**

1. Please fill in the bank name as XXX bank XXX branch XXX sub-branch in Chinese.
2. "Account Holder Name" is mandatory filed. Chinese employee need to fill in your Chinese name.

If any issue occurred during filling in the bank information, please contact with ASKHR team askhr@microsoft.com.

Each employee only can hold one reimbursement account. All of your reimbursement payments will be paid to this reimbursement account. So if your current reimbursement account is not ICBC/AMEX card, please note to make money transfer by yourself.

Contacts of T&E related question

MS China AP

[P2P Support Portal/ Finance Digital Assistant](#) (FDA) - [guidance video](#)

Hot Line: +86 400-650-2418

VIII. MICROSOFT REAL ESTATE & FACILITIES SERVICES

Main Reception

The main Reception services include visitor reception and registration, phone transfers, large conference room reservation and coordination, luggage storage service, handing out mask, lanyard and badge cover, and temporary badge borrow and return. Besides, the receptions for some sites are responsible for F&B ordering, stationery service, Business card/meal card/SIM card/4G card picking up, expense reports collecting assistance and temporary card management, collecting back badges from terminated employees etc.

Employee Meal Service

For Beijing West site, RE&F will recharge the meal allowance for new employees based on the on-board notice. Meal card (badge) it can be used at Main Canteen at Tower1-3F, Beijing Courtyard, Bing-Go, Micro Bistro, Spring Bloom at Tower1-2F, Papa John's, Starbucks, Micro Supermarket at Tower2-3F, and various F&B markets at campus.

The meal allowance mode for Beijing West FTE will be two options for you to choose from as follows:

Meal card (badge) allowance or Salary meal allowance

The meal allowance mode can be selected only once a year. Once selected, it cannot be changed till the following year. You will receive this email at the end of each year to select the meal allowance mode for the following year. If we do not receive your selection before the deadline, we will keep your current allowance mode.

1. In Beijing, about meal card function freeze, activation, subsidy and other related questions, please send email to the dining service public mailbox: bjdining@microsoft.com
2. On the day subsequent the terminated employee's departure, the meal card function of the badge will be frozen, and the remaining balance in the card will not be refunded.
3. The subsidy of new employees in the onboarding month will be issued to the badge according to the onboarding date. Fixed recharge time of subsidy is the first week of each month.
4. You will receive the meal allowance at the end of the previous month or the beginning of the month.

For Shanghai ZiZhu Site, RE&F will prepare and recharge meal cards for new employees automatically at a fixed time every month according to the onboarding notice. When you receive the meal card collection email, you must bring the relevant documents to the designated location to pick it up (Shanghai Zizhu B01/B07-5F front desk). The meal card can only be used in the B05/B07 canteen and the B01 lobby coffee bar. There are two allowance mode for you to choose from "Meal Card Subsidy" and "Salary Subsidy". Once chosen, it cannot be changed till the following year. We will confirm your choice every January through email till the 3rd working day, if not so, we will keep your current allowance mode. If you have any questions on meal allowance, please send an email to svlzzrec@microsoft.com.

For Shanghai HUAXIN site, the meal allowance will be paid through your payroll. If you have any questions, please send an email to shhxref@microsoft.com.

For Shanghai MSRA site, the meal allowance will be paid through your payroll. If you have any questions, please send an email to shairef@microsoft.com.

For Guangzhou site, meal allowance will be paid along with the monthly payroll.

FTE meal subsidy model in other cities will be decided by the local Finance Department.

Office Equipment

Office equipment include public shredders etc. RE&F team has posted the equipment usage guideline for proper operation and maintenance. If you have any question on copy service, please contact RE&F Global Facilities Service Center Helpdesk for help.

Stationery Service and Business card

- Stationery service is managed by local RE&F team.
- Common stationery such as envelop, and paper bag are available in the Utilities Area on each floor.
- For special or specific items, please contact the floor captain in Beijing or contact the local reception desk for other offices.
- Bulk stationery for special intention or event is ordered by the team AA and charged to group cost centre.
- Employees should apply for the business cards via RE&F platform and the online name cards application website is
- <http://ref.chinanorth.cloudapp.chinacloudapi.cn/namecard/en-US>

For any query on this website, please contact

Beijing: bjcrefsc@microsoft.com

Shanghai Zizhu: svlzzrec@microsoft.com

Shanghai Huaxin: shhxref@microsoft.com

Shanghai MSRA: shairef@microsoft.com

Suzhou: szref@microsoft.com

Wuxi: wuxifm@microsoft.com

Nanjing: njref@microsoft.com

Shenzhen COMTECH: prcgzfm@microsoft.com

Guangzhou: prcgzfm@microsoft.com

Mail Service

In Beijing office, Shanghai Zizhu Campus, Shanghai Huaxin office, Wuxi office, Suzhou Campus and Shenzhen COMTECH, there are one mail rooms and dedicated mailers in charge of all mail services. The mailer will deal with all incoming and outgoing mail items such as international, domestic, urban express delivery services, ordinary mail and domestic parcel delivery. The contact number are:

- Beijing: ext. 79009
- Shanghai Zizhu: ext. B01 – 83334, B07 - 80007
- Shanghai Huaxin: ext. 89213
- Shenzhen COMTECH: ext. 8050
- Wuxi: ext. 8801
- Suzhou: ext. 8080

For other cities, the reception is responsible for local mail service.

Before you send out your mail item, please submit the request via RE&F platform and online

mailing service. For any private mail, postage expenses will be undertaken by themselves. The application website: <http://ref.chinanorth.cloudapp.chinacloudapi.cn/Mail/en-US>

All the incoming express mail/packages, the mailer or receptionist will register, and deliver to you or contact you to pick up. Normally, you are required to sign the registration book for EMS, DHL expresses or registered letters. Bulk express delivery services for large-scale event should be ordered by team AA and a raised PO is required in MS Market system.

Internal office mail: if you want to deliver any documentation within same office, you can ask office assistant assistance.

Office Space Management

According to the headcount of next financial year forecasted by Microsoft China, RE&F will proceed seat allocation and office expansion plan and submit to management team for final approval during April to June each year, the period of Microsoft global budget. The RE&F team will also allocate seats for new employees during the daily work. HR department will send new employee announcements to the related departments; facility management team of every site will coordinate with assistant of every department to arrange seats in accordance with Microsoft policies and the actual situation of the existing seats.

To ensure seating arrangements are more effective and fully consistent with the company's financial, auditing, taxation, personnel and legal policy requirements, the facility management team won't accept the following or similar applications:

- Any non-Microsoft (china) employee can't have private office at Microsoft (China) office buildings. If anyone has such requirements for work-related reasons, he/she can book a meeting room as a visitor.
- Any Microsoft (china) employees can only have no more than one fixed seat in Microsoft (China) offices. If anyone needs to work in other offices temporarily, he/she can book a meeting room as a visitor or share seats with Local colleagues.

In-Office Move Service

Where staff wishes to move to a different workstation or are required for operational efficiency to move to a new workstation, please inform RE&F team after obtaining approval from your Business manager.

The RE&F team will arrange with the relevant services for moving your stuff to the new location and other related technology changes if necessary.

Pantry Services

There are drinking water dispensers and coffee, milk, Chinese tea, soft drinks, biscuits and instant noodles in each floor's pantry.

The consumables in the pantry are replenished regularly.

For any assistance, RE&F Help Desk (See Below) or related person.

Incident Reporting

All accidents, no matter how minor, should be reported to local RE&F team.

Current guidelines for dealing with accidents are:

- Please pay particular attention to dealing appropriately with any incidents or accidents involving staff or visitors. They must be reported promptly and in full to the RE&F team.
 - Act promptly and sympathetically in case of injury or shock, taking note of how the incident occurred, details of the victim and witnesses, and reporting the incident immediately.
 - Seek appropriate treatment urgently. Call public emergency phone number **110/120** for help.
 - For there is any loss or damage to the company assets or employee belongings,, please report it to to the company assets or employee belongings,:
<https://microsoft.sharepoint.com/sites/security/Pages/ReportItNow.aspx>
-

Facility Management Service Information

If you have any RE&F service requests and queries, please send an email to the below alias for help:

- Beijing: bjwref
 - Shanghai Huaxin: shggwref
 - Shanghai Zizhu: sh-zizhu
 - Shanghai MRS: shmrsref
 - Shanghai MSRA: shairef
 - Guangzhou: prcgzfm
 - Shenzhen: prcszfm
 - Wuxi: wuxifm
 - Suzhou: szref
 - Nanjing: njref
 - Chengdu: prccdfm
 - Chongqing: prccqfm
-

RE&F Global Facilities Service Center Hotline

The Facilities Help Desk is to provide quick responses to your facility-related requests. You can unify dial +12067774702 or search "MSFacilities" on Teams and dial directly.

Please call **Helpdesk** for following service:

- Office facility services such as lighting, electrical, air conditioning and plumbing.
- Cleaning service.
- Food/Beverage/Snacks and pantry services.
- Office maintenance and repair service;
- Furniture or box moving service.
- Mail service.
- Storage Room service.
- Office equipment service.
- Conference room set up and tea service.
- Environmental, health and safety.
- Indoor planting service.

For more updated and detail information about local RE&F service, please link the website below to download the facility manual of your office:

<https://microsoft.sharepoint.com/sites/refwebhub>

IX. Microsoft Digital (formerly Microsoft IT) HANDBOOK

Microsoft IT has been changed to **Microsoft Digital**

Microsoft Digital Service

The Mission of Microsoft IT is to delight our customers by providing the most dependable, high value, trustworthy technology services and to continually improve the experience for visitors of **TechWeb**, while using Microsoft technologies.

You can start with <https://aka.ms/techweb> to find the support method that works best for you.

- 1) Chat with Virtual Agent to get 24 hours online technical support:
<https://aka.ms/gsvirtualagent>
- 2) Global IT Service Desk

Office	Language	Internal Dial	External Dial
Beijing	English & Mandarin	75000	400-8675000
Shanghai	English & Mandarin	85000	
Shenzhen/Guangzhou/ Chengdu/ Nanjing/Jinan /Hangzhou/Suzhou/Wuxi	English & Mandarin	5000	
Others	English & Mandarin	-	

- 3) Digital TechLink: <https://aka.ms/digitaltechlink>

System Initial Settings(More details, you can refer to <https://aka.ms/iamnew>)

[Step 1, Set up your account](#)

[Step 2, Set up your computer](#)

[Step 3, Set up your mobile device](#)

Set up your account

1. Reset your Initial Password

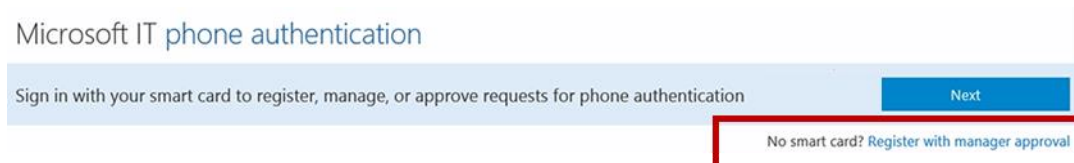
- Your direct manager will provide you with your account and your initial password. You might need to reset your password when you sign in your pc first time with corpnet connectivity. If you are remote onboard, you can visit this website to reset your password: <https://msft.sts.microsoft.com/adfs/portal/updatepassword>.
- Please refer to this password guidance to create a strong password: [Guidance for setting a strong, and unique password \(sharepoint.com\)](#)

2. Phone Authentication

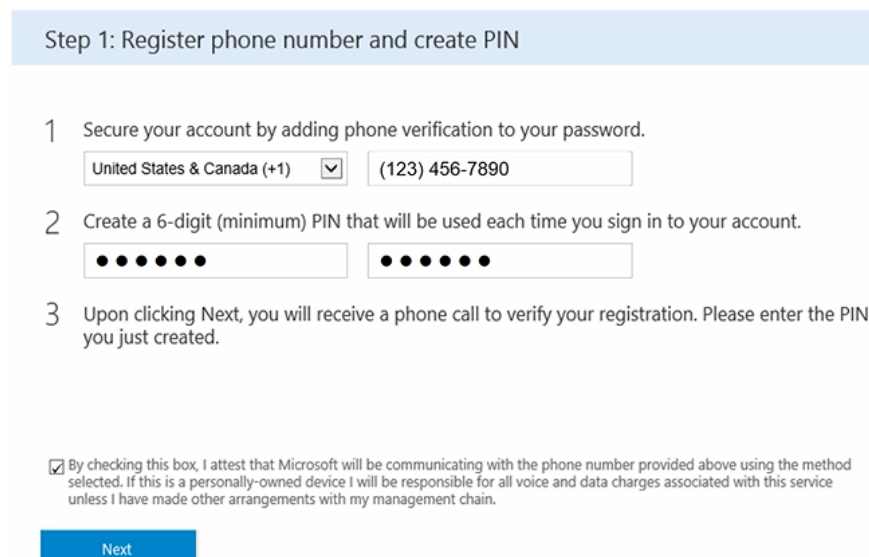
Built on [Azure Multi-Factor Authentication](#), the Phone Authentication service enables you to easily access corporate resources from anywhere, at any time, on a variety of devices, even when you don't have your physical or virtual smart card available. It is a key enabler for the Secure Logon experience with 2-factor authentication that allows you to connect to a variety of corporate resources including Microsoft 365, Azure sites and remote connectivity solutions without needing a smart card.

How to register for Phone Authentication:

- a) Access the link on your PC <http://aka.ms/ringring>, then select "Register with manager approval"

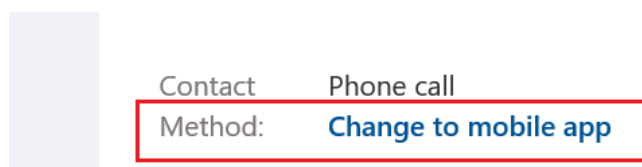


- b) Input your mobile phone number and create a 6-digit PIN. Then select check box and click "Next".



- c) You will receive a call, please answer the call and and with "#" to confirm.

Note: Each time when you use the phone authentication services, you will be asked to enter a 6-digital PIN number. If you don't want to receive a call every time, you can change the authentication method to Mobile App. If you are now using a China Android OEM mobile device, you might have to use phone call method instead due to most China Android devices don't support Google Mobile services. You can swift authentication contact approach via <http://aka.ms/ringring> as illustrated below.



Set up your computer

We use the standard software environment:

- Microsoft 365 (Windows 11+Office 365)
- Bitlocker enable to protect your data
- Set up printer driver and login

As a Microsoft employee, we are the first and best customers to Microsoft products and solutions. Microsoft Digital team advocates you to be familiar with our first-party products and solutions by starting to set up your working machine.

In general, your working machine will be available on which date you are onboard. After you power on your machine, you can refer to this document for how to provision your machine:
<https://iamnew.powerappsportals.com/computer-setup/>

Notes:

- Due to asset management policy is different from business to business, here we just use the scenario you have a new device as an example. If your scenario is different, you can dial in 400-867-5000 for help via your mobile phone.
- During the provision, you might need a secure network connection. If you are at home, then please connect your device with your home broadband. If you are in the office, you might need to connect your device with MSFTGUEST. About how to connect with MSFTGUEST, you can refer to:
https://microsoft.sharepoint.com/sites/Network_Connectivity/SitePages/Wireless/MSFTGUEST.aspx
- If you meet any questions during the provision, you can dial in 400-867-5000 for help via your mobile phone.

Once you have configured your machine, we will walk through with you the applications/solutions you need to use daily, they are:

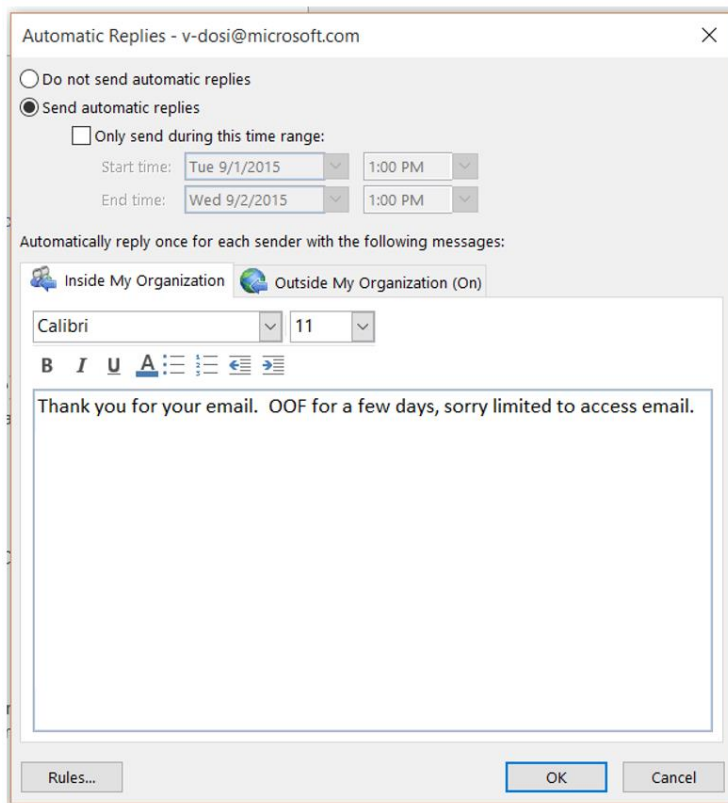
- **Microsoft Outlook**
- **Microsoft Teams**
- **Microsoft BitLocker**
- **Printing settings**
- **Microsoft OneDrive**
- **Remote Access Services**

Setup Outlook

- 1) Open Outlook, click "Next" on the welcome window, select "Yes" on Accounts setting and click "Next".
- 2) Outlook will search your name and email address automatically, and then click "Next"
- 3) After the email profile Configuration, click "Finish"
- 4) You can also sign in your mail box via Outlook Web App(OWA):
<https://outlook.office365.com>

Set up Out of Office Assistant(OOF)

- 1) Open the **File** Menu, click **Automatic Replies**.



- 2) Select **Send automatic replies**.
- 3) Type the OOF message content.

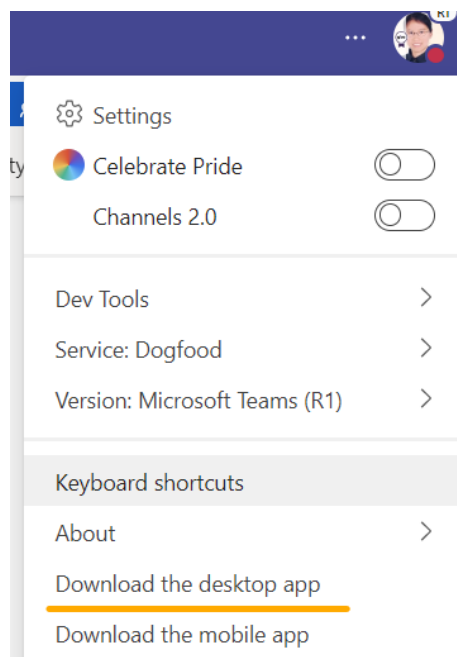
Note: You can also turn on your Out of Office Assistant from Outlook Web Access (OWA).

Collaboration tool - Microsoft Teams

Microsoft Teams is the chat-based workspace in Microsoft 365. It's a true hub for teamwork and can be customized to fit your team's needs. Microsoft Teams is flexible for chats, calls, meetings and sharing files.

How to get Microsoft Teams

1. Visit Microsoft Teams website through this hyperlink: <https://teams.microsoft.com/> to get desktop version downloaded. (Settings>>Download the desktop app)

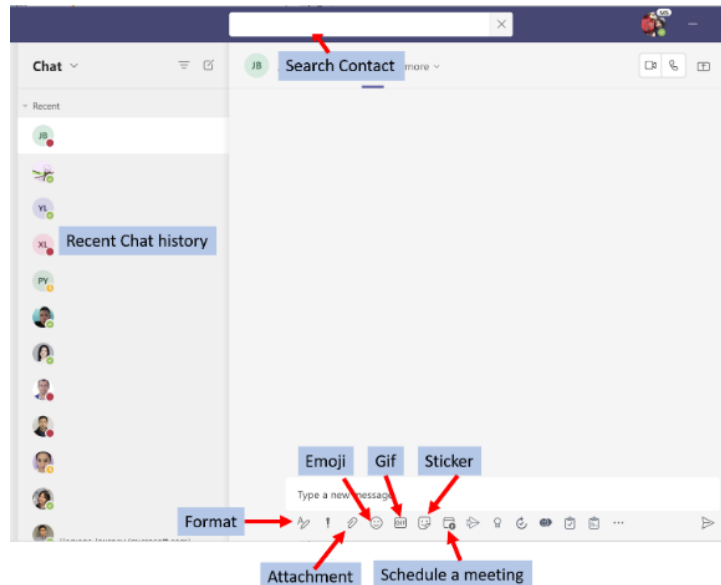


Get started with Microsoft Teams

1. Chat

You can follow the below guide to start your conversation in Microsoft Teams:

[Chatting in Microsoft Teams \(sharepoint.com\)](#)



2. Enterprise Voice Phone System

With Phone System, users can use Teams to place and receive calls, transfer calls, and mute or unmute calls. You can follow the below guide to use the phone function in Microsoft Teams:

[Calling in Teams \(sharepoint.com\)](#)

- To ensure your call quality, please use headset Microsoft Teams authorized to make calls and join Teams meetings.
- You can submit your EV application by visiting <http://aka.ms/phonerequest>.

3. Meeting

How to organise and join Teams Meeting

Join Teams meeting through Teams hyperlink in the meeting invitation.

Microsoft Teams meeting

Join on your computer or mobile app

[Click here to join the meeting](#)

Or call in (audio only)

[+86 400 819 0802,,161473329#](#) China, All locations

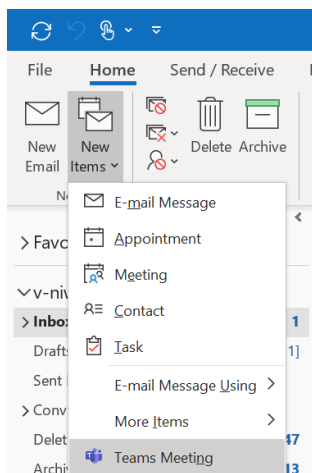
Phone Conference ID: 161 473 329#

[Find a local number](#) | [Reset PIN](#)

[Learn More](#) | [Meeting options](#)

Note: Please watch out correct the dial-in number (400) in the meeting invitation (the local number can be found out in Find a Local-number option)

4. Start a Teams meeting through Outlook

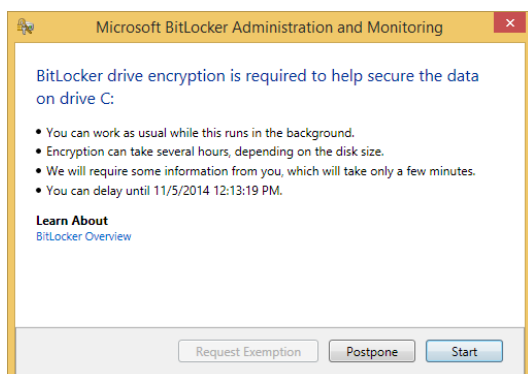


5. You can follow the below guide to learn how to join and organise meeting in Microsoft Teams:
<https://microsoft.sharepoint.com/teams/Meetings/SitePages/Hybrid-meeting-guide.aspx>

Protecting Your Data with BitLocker

Microsoft BitLocker Drive Encryption technology uses the strongest publicly available encryption to protect your computer's data and prevents others from accessing your disk drive(s) without authorization.

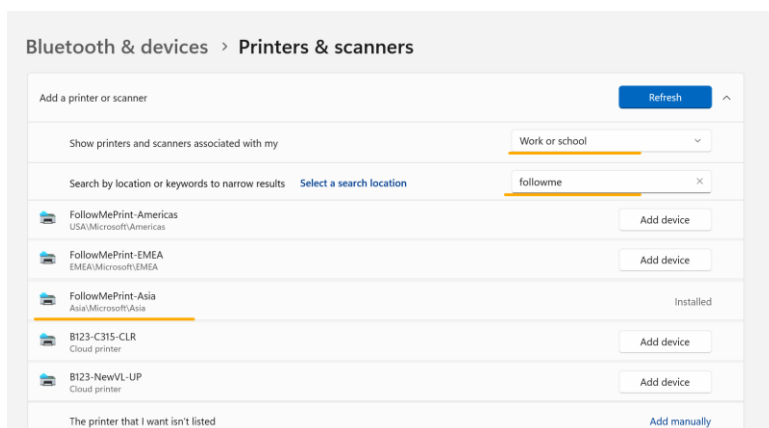
When you install Windows 10 or Windows 11, you can use the Setup program to enable BitLocker. If you did not enable BitLocker during the installation process, you can refer the picture as below to enable it to protect your data. (Control Panel → BitLocker Encryption Option)



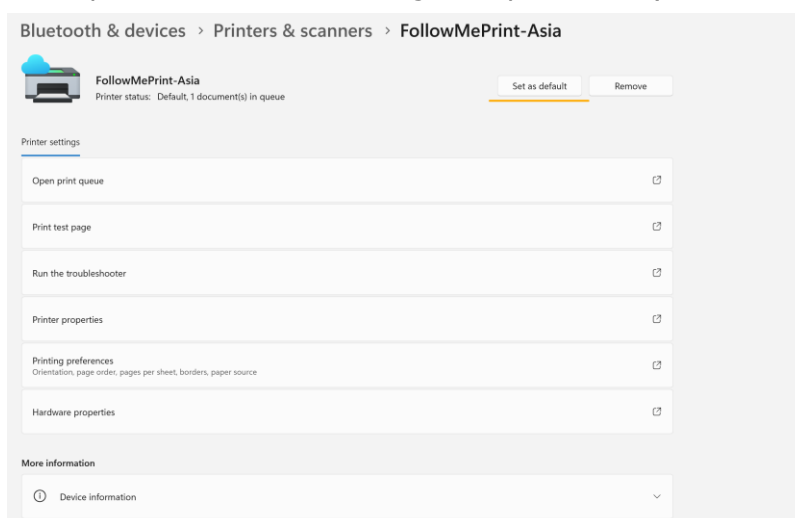
Note: The encryption process takes some time depending on the size of the disk C, please plug in the power. During this period, the system can be used normally.

Connect to Network Printers

1. Go to Windows "Settings" (Right click Windows logo, and click "Settings")>>"Bluetooth & devices">>"Printers & scanners">>"Add device"
2. Select "Work or school" and key in keywords as "followme", and pick up "FollowMePrint-Asia" and click the button "Add device"



3. After printer driver being installed, you can set this printer as your default device by clicking this printer and click the button "Set as default". BTW, you can use this printer when your device is connecting to any network (no need to connect "MSFTVPN").

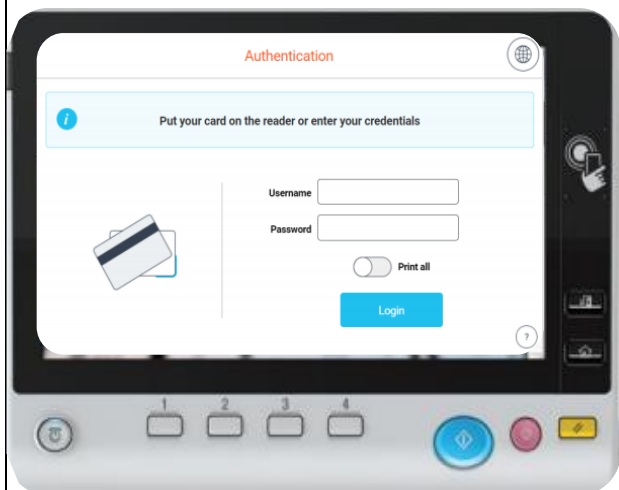


When first time use the printer, please make the registration (after the completion of registration, you can use all Asia printers, etc TW, HK...). The procedure is below:

1. Swipe your Microsoft ID card on the printer
2. Enter your Microsoft alias and password
3. Click "Activate" button

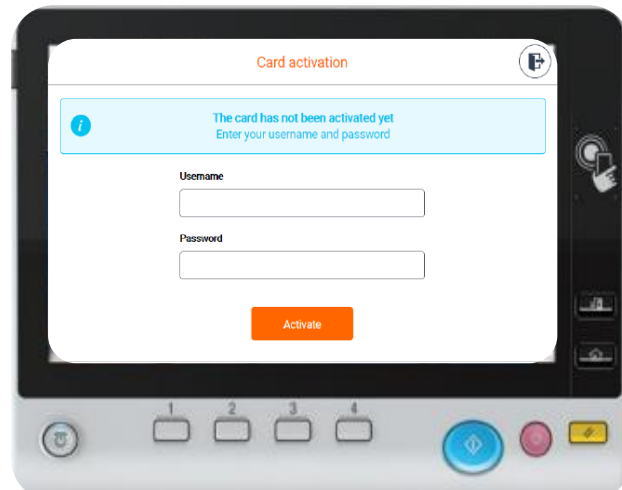
Authentication Screen

Swipe your Microsoft ID card on the printer, the authentication windows pop up.



Activate

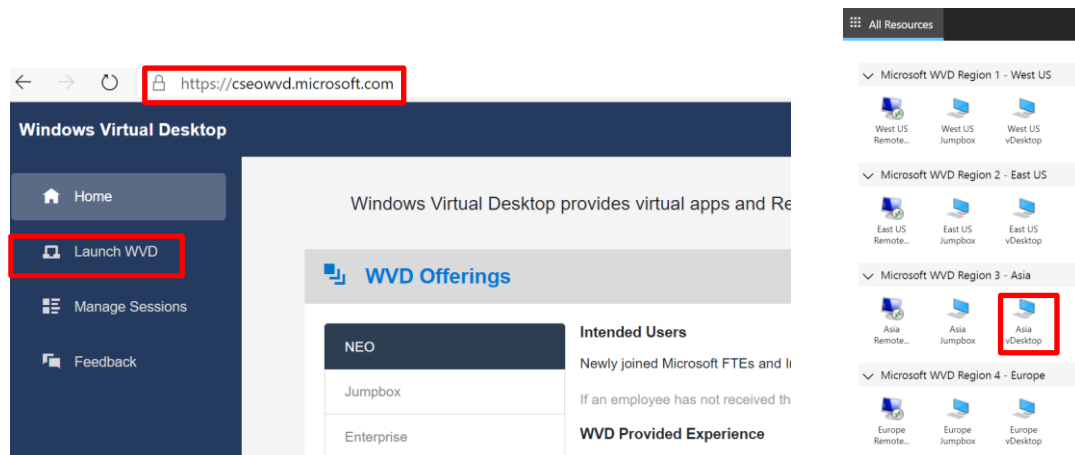
Enter your Username (Alias) & Password, then select "Activate" to finish the registration.



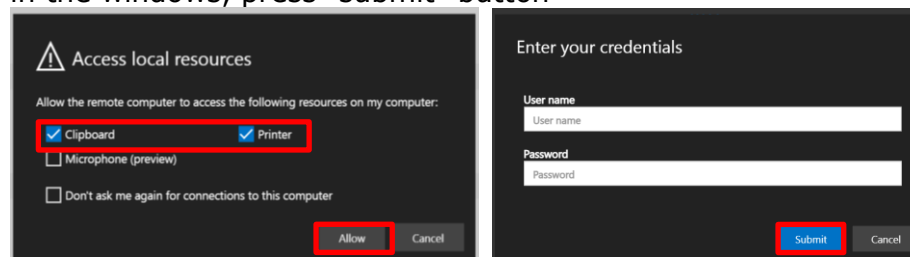
Noticed :

1. You can use WVD (Windows Virtual Desktop <https://cseowvd.microsoft.com>) to install the printer too, the operations details listed below:

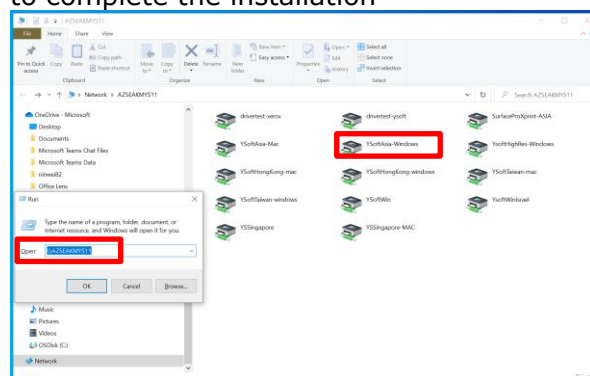
Goto aka.ms/CSEOWVD ,Select "Launch WVD", then as windows pop up, select "Asia vDesktop"



Leave the default selections, Press "Allow" button. Then to enter your alais and password in the windows, press "submit" button



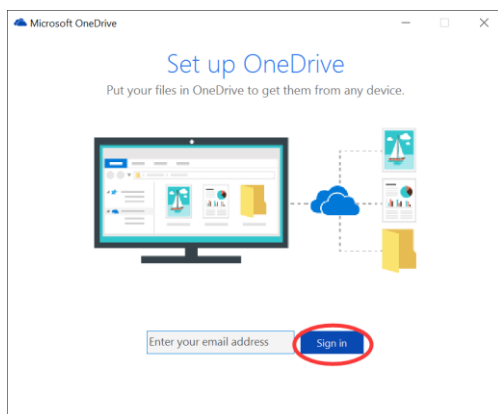
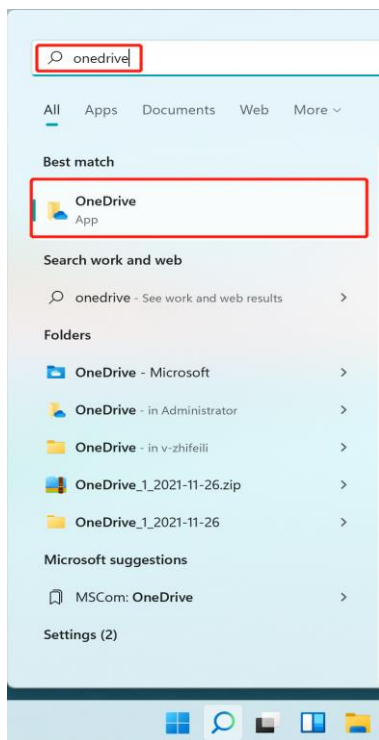
Enter "windows" + r, then enter\\AZSEAKMYS11, select and double click "YSoftAsia-Windows" to complete the installation



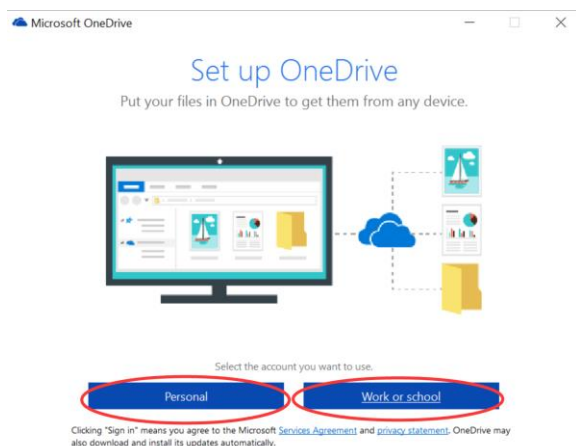
For further assistance, please contact Global IT Service Desk.

OneDrive - Use Document Library in the Cloud

1. Search "OneDrive" from the left of taskbar (Online Link: <http://onedrive.com>)



2. Click "Sign in" to the follow dialog



Use your alias to sign in "Work or school" account, you can store our functional spec, project plan, or other work-related materials. You may store Highly Confidential information on **OneDrive -Microsoft**, if you apply the right protection to your files. More about OneDrive, please refer to:

<https://microsoft.sharepoint.com/sites/Collaborate/SitePages/Set-up-OneDrive-and-start-syncing-your-files.aspx>

Use your Microsoft Account to sign in your "Personal" account, you can store your personal documents like Mom's chili recipe or pictures of the kids. Don't store any Microsoft business documents on OneDrive – Personal!

Remote Access Service

Remote Access Service (RAS) is a broad term for the services and connections that enable you to connect remotely to the Microsoft corporate network from outside locations such as your home, hotel room, customer, or business partner networks.

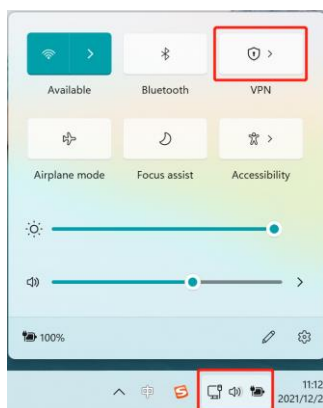
You can use [MSFTVPN](#) to connect corporate network on Windows 10 or Windows 11 system.

Set up Phone Authentication ([View more](#))

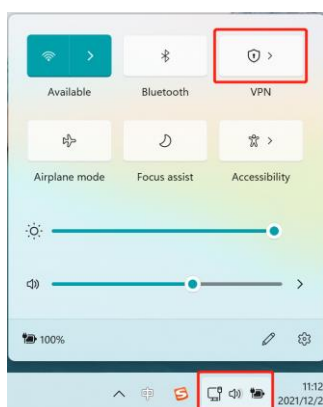
Phone authentication is a phone validation service which is based on Azure Multi-Factor Authentication and can allow you to visit Microsoft internal resource no matter when and where on any device. Please set up you phone authentication ASAP, which can help you log in O365, Auze and remote connection.

Using MSFTVPN to visit Microsoft internal resource

1. Click 'Notificatoin Center' on the right corner of taskbar and press 'VPN'



2. Choose 'MSFTVPN' then click 'Connect'



Anything above you need, please contact Global IT Service Desk or visit <https://aka.ms/rasrequest>.

Set up your mobile devices

Microsoft offers various solutions to allow your mobile devices to access Corporate resources.

You can pick up the optimal one to fulfill your needs. More details, please refer to: https://microsoft.sharepoint.com/:w:/r/sites/CSEOChina/ layouts/15/Doc.aspx?sourcedoc=%7BE8E75A24-7256-4BF9-8AED-A7A88F92C160%7D&file=Guidance%20of%20Modern%20Access.docx&action=default&mobileRedirect=true&share=IQEkWufoVnL5S4rtp6iPksFgAZwLDIh_hXOUKLWB3-VAjIM

About Microsoft Network Environment

How to prevent the network port from becoming disabled

Your network port is scanned every day. If your machine is suspected to be compromised, such as virus, lack of critical updates or connected to wireless AP, the network port connected will be disabled and you will have no access to any network resources.

Wireless connection

In continuing the Consumerization of IT (COIT) effort, Microsoft IT will segment wireless network traffic by separating domain joined devices and non-domain joined devices.

The following domain-joined devices are allowed to connect to **MSFTCONNECT**:

Any device which has joined AD or AAD will connect with MSFTCONNECT automatically. Please manually switch to MSFTCORP if you like to use it.

- Windows 10 / Windows 11 and Windows Server 2016/2019

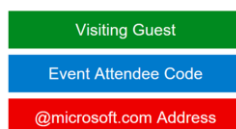
Windows 8 and Windows Server 2012 In addition, the following Intune-enrolled devices are allowed to connect to **MSFTCONNECT**:

- Windows 10
- Windows 11
- IOS 15.1 and higher
- Mac OS X 10.15.7 and later
- Android 10.x and above

Non-domained joined PC devices may connect via **MSFTGUEST**, Please connect to MSFTGUEST and select one of the following login methods.

MSFTGuest Login

Please select one of the following login methods:



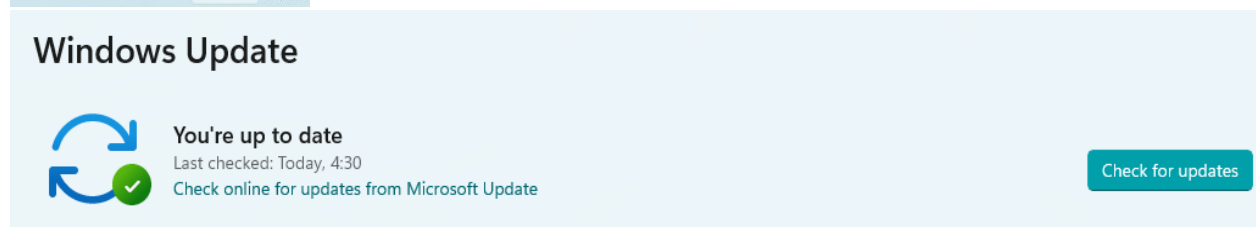
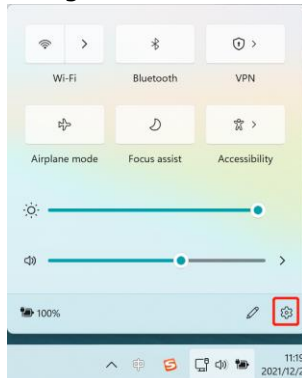
Non- domained joined mobile devices, connect to **MSFTGUEST** and visit the <https://getconnected.microsoft.com/>. Then please select one of the above login methods.

Please note your mobile device must enroll MS Intune if you need it to access corporate resources, such as accessing Outlook mobile client or signing in Teams mobile client for

communication by following information security requirements. In the meantime, your device needs to install and activate Microsoft Defender for Endpoint (MDE) for protection. For more information about intune-enrolled, please visit: <http://aka.ms/device-enrollment>

Windows Update

Please check and install the Critical Updates in Windows Update to prevent the port from being disabled.



Microsoft Information Services General Use Standard

Do and Do Not

- 1) Encrypt High Business Impact (HBI) information at all times
- 2) Lock your computer when you step away (Windows + L key)
- 3) Keep your Operating System (OS) and all applications up-to-date
- 4) DO NOT share passwords or credentials with anyone
- 5) DO NOT install unapproved Peer-to-Peer (P2P) applications or any freeware
- 6) DO NOT leave laptop or mobile devices unattended

Proper using Messaging Services

- 1) Instant Messaging (IM) – transfer unprotected information only, no Confidential/ High Confidential. For business usage. Do NOT talk political and erotic topics
- 2) Approved IM software: Microsoft Teams Skype for Business and Skype
- 3) Avoid large group broadcasting. Be careful of using "Reply to All"
- 4) Do NOT forward Microsoft emails outside of Microsoft or third part destinations

For further more, please refer to

<https://egrc/foundation/Workspace.aspx?workspaceId=&requestUrl=>

Related Web Sites and Software Installation

- Please Start Software Center, search the software and install it.
- Tech web: <https://aka.ms/techweb>
- Self-reset Password: <https://sspm.microsoft.com/>

X. MICROSOFT GLOBAL SECURITY INSTRUCTION

Access Control

Microsoft has hundreds of buildings worldwide that house Microsoft people, data, and assets. It's important that we all do our part to keep them secure - controlling building access is everyone's responsibility. Microsoft uses access control systems to limit building entry to authorized personnel. This helps maintain a safe work environment and restricts access to sensitive business information and Intellectual Property.

What determines the type of access control for your office or building? Access control is applied based on geographic risk (e.g. physical location of the office or known/potential Security threats) and business risk (e.g. Intellectual Property development or the presence of Senior Management).

Responsibilities for access card and access management are handled by Global Service Access Management (<https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Services-GSAM.aspx>).

Access Card

Your access card is pre-programmed with access to your normal contracted place of work. If visiting other sites or intend to work at other sites for a period of time:

visit -GSAM Self-Service Portal tool (<https://aka.ms/gsamssp>). The tool allows Microsoft employees and contingent staff to self-manage physical access cards and smart cards for logical access needs.

If you lost your access card, please take these actions:

1. Visit GSAM Self-Service Portal tool (<https://aka.ms/gsamssp>) to deactivate a lost card, reactivate a found card or report a stolen card.
2. While your new badge is being processed, go to Microsoft reception or GSAM (if available) to apply for a temporary badge.

Access Control Tips

- Always wear your access card in full view at work - those who don't belong will stand out.
- Refrain from holding open secured doors for others to help deter "tailgating." Tailgating is the easiest way for unauthorized people to gain access.
- Challenge tailgating attempts. If you are met with uncooperative or hostile behavior, contact Site Security, Global Security or your Security Point of Contact immediately. [Click here](#) to see respectful ways you can challenge tailgating attempts.
- If applicable at your site, swipe your access card each time you enter a secured door and require coworkers to swipe their access cards. In the event of an emergency, you will be included on the list of employees who may still be present in the building/office.
- Never lend your access card or work keys, and report missing cards and work keys to your Security immediately.
- Instruct coworkers who have forgotten their access cards to obtain employee non-escort temporary pass from reception as appropriate to your site.
- Shut entrance, exit, and lab doors behind you, and lock doors whenever you leave. It could take less than a minute to enter your workspace, take something, and leave the building.

- Secured doors should only be propped open when a delivery is in progress. At all other times, these doors should remain closed and secured.
- Follow visitor procedures so that those who don't belong will stand out. If a guest does not have a visitor pass, escort them to reception where they may obtain one.

Visitor Management Procedure

Microsoft devotes numerous resources to protect those things it values most - its people, data, and assets. Receptionists, secured doors, card readers, and access policies are only as effective as the people that make use of them. It takes only one person to put everyone in jeopardy. Remember, safety and security at Microsoft starts with each of us.

Each Office Has Visitor Access Procedures. Stick to Them!

(<https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Awareness-AccessControl-Visitors.aspx>)

- All visitors must be met by an employee at the main reception area or main lobby.
- Visitors must present valid picture identification for sign/check in.
- Visitors should receive and display a visitor pass, valid only for that day.
- The pass should clearly show the expiration date and areas where it is authorized.
- Visitors must be escorted at all times while in secured areas.
- The pass must be returned, and the visitor should sign/check out.
- After-hours and weekend visitors should be approved by the employee's manager, and Global Security should be informed.
- Visitor passes may only be issued for up to five consecutive days to the same person.

Visitors Include

- Personal guests, including family members & children
- Class attendees
- Survey/Test Group subjects
- Conference guests
- Consultants

Make No Exceptions for These Services - Employees should personally meet these people in the lobby

- Caterers
- Couriers
- Fast food deliveries
- Floral deliveries

Theft Prevention

From time to time, exploits to our work setting occur, including theft. Those seeking to take advantage of our environment need two things to succeed - opportunity and access. Follow these physical security best practices to help prevent theft and keep our workplace secure.

Limit Opportunity

- Avoid bringing valuable personal items to work.
- Use lockable drawers, cabinets, and closets to store valuables.
- Hang coats and sweaters away from entrances to your office/workspace, and hang them

out of sight.

- Keep briefcases and handbags out of public view. Lock them up if possible.
- Secure all keys to offices, cabinets, drawers, storage areas, and docking stations.

If you are going on vacation, do not post your absence on your office door or department white board. Instead, set your Outlook "Out of Office Assistant" and update your voice mail.

- Keep your desk clutter free, and clear your desk before you leave work for the day. Your work space will be less appealing to an intruder, and if anything is missing it will be more obvious.

Tighten Access

- Never prop open entrance, exit, or lab doors. It could take less than a minute to enter your workspace, take something and leave the building.
- Wear your access card in full view at all times. If you see someone without an access card or visitor pass, ask who they are and direct them to the receptionist. If you're uncomfortable, call your local Security and Global Security.
- Follow visitor registration procedures. Instruct your guest to bring picture ID, and personally meet them in the lobby. Remind guests to display their visitor badges, and escort guests at all times.
- If someone shows up unexpectedly and says they are a repair person or vendor, ask for their identification. If you're unsure, ask your manager or contact your Facilities group.
- Always use your badge to enter secure doors, and never hold a secure door open for anyone.
- Make sure doors are closed and locked before you leave for the day.
- Be especially aware of activity in your area after hours and on weekends. You're more likely to be alone, and therefore, more vulnerable.
- Never lend your work keys or access card to anyone, and immediately report lost keys or access cards to your manager.

If a Theft Has Occurred

Report all thefts to your local Security and Report It Now <https://aka.ms/ReportItNow> (click "submit a Physical Security report" button) so that the theft can be recorded and investigated appropriately by Global Security.

As detailed in Microsoft Risk Management

(<https://microsoft.sharepoint.com/teams/riskmgmt/Pages/Personal.aspx>), Microsoft assumes no liability for loss, theft, damage or destruction to any personal property that an employee may have at Microsoft or while traveling on business. If employees wish to bring personal articles to Microsoft, they do so entirely at their own risk. Microsoft may, however, agree to compensate an employee for their personal property loss if both of the following conditions are met:

- The employee has been requested in writing by his/her manager to bring the property to Microsoft for use on Microsoft-related work, and that request is executed prior to the occurrence of the loss.
- In addition, it must be proven with reasonable certainty that any ensuing loss or damage was the result of negligence or carelessness on the part of Microsoft or Microsoft employees acting in the scope of their employment, and not caused by the carelessness of the employee. Unlawful activity by other employees or vendors does

not constitute Microsoft carelessness or negligence.

If members of your group are concerned about the risk to their personal property at Microsoft, they should consult with their personal insurance agent to assure their homeowner's or renter's coverage will extend to their belongings at Microsoft.

Personal Safety

It is important to remain vigilant about your personal safety to and from work, and when you conduct business off-site. Incidents of violence can occur anywhere at anytime.

Mind Your Attitude! Never underestimate the power of your attitude. How you perceive a stressful situation will impact your ability to act. It's imperative that you remain as calm and level headed as possible. Try to channel your nervous energy into a solution-focused mindset.

Recommendations

- Be alert and aware of your surroundings at all times.
- Know building access and exit points.
- After office hours, use the buddy system.
- Practice safety precautions at the office, on the go, and at home.
- Know how to contact security.
- Trust your instincts.
- Ask directions only from persons in authority.
- Do not accept food or drink from strangers.
- If you feel uncomfortable, move away from the source and move quickly towards safety.
- Do not enter a confined space such as a restroom or elevator if someone inside makes you feel uncomfortable.
- When traveling, avoid fatigue. Rest, drink plenty of water (bottled water if you're unsure about water quality) and eat a healthy diet.

More personal safety prevention tips available at:

<https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Awareness-PersonalSafety.aspx>

Emergency Preparedness

Microsoft has developed programs and processes to help employees be prepared in case of a disaster. Sometimes there are warning signs of these impending events, and advance preparation and awareness can minimize their impact. Other times they strike with little to no warning.

Educating yourself in precautionary measures and knowing what steps to take when an event occurs is a responsible step toward helping protect you and your family. We strongly encourage all employees to participate in the emergency preparedness drills conducted annually at their sites. In addition to knowing the emergency contact numbers within your area, know the evacuation routes and precautions to take during evacuation and locating shelter.

Update Your Contact Information

In case of an emergency, Global Security will communicate via email and/or SMS text to employees in the affected region.

We ask for your help to ensure Security can communicate with you to conduct welfare status checks during emergency situations.

Full-time employees can manage contact information through [HRWeb](#).

Providing mobile phone number is voluntary; should you decide not to, Security will attempt to reach you via email. SMS texts are delivered to the primary number listed in HRWeb. This field by default also publishes to the Global Address List (GAL). We understand the need for privacy, and have updated guidance based on your country (please see additional information below).

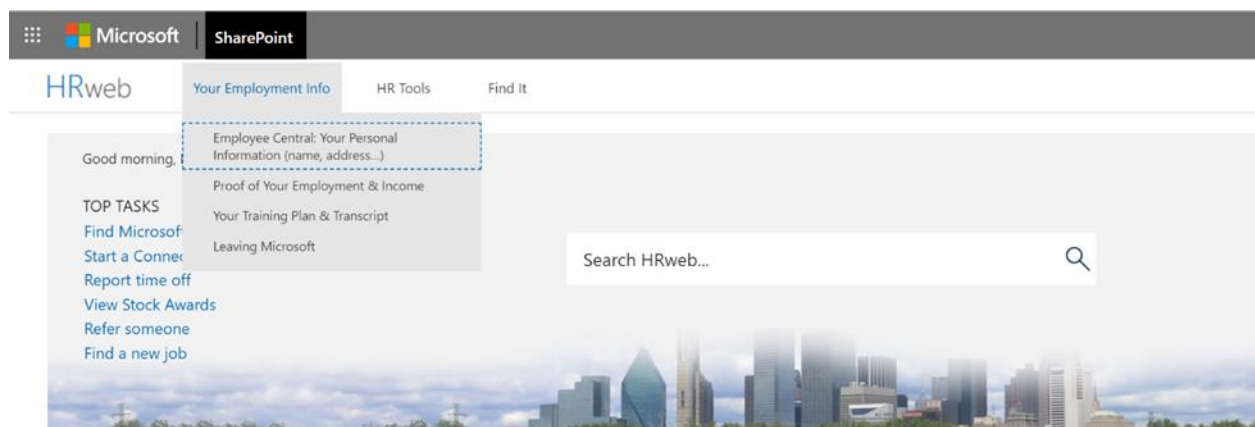
Update your details by following these steps:

1. Navigate to [HRWeb](#) to update your contact information.

2. To learn more on this process, [visit this document link](#)

([https://microsoft.sharepoint.com/teams/Emergency_Preparedness/Shared%20Documents/Update%20Contact%20Info/FTE%20Update%20Contact%20Info%20\(1\).pdf](https://microsoft.sharepoint.com/teams/Emergency_Preparedness/Shared%20Documents/Update%20Contact%20Info/FTE%20Update%20Contact%20Info%20(1).pdf)).

* Privacy Note: By default Security SMS texts are delivered to the number listed in HRWeb as "Work Mobile (GAL)". This field is also published to the Global Address List (GAL). If you do not wish to have your primary contact number displayed in the GAL, but would still like to be contacted via SMS, please include your number in "Work Mobile (Private)" field.



Microsoft Global Security Emergency Preparedness Site:

https://microsoft.sharepoint.com/teams/Emergency_Preparedness

Travel Safety

Microsoft is committed to employee safety through its travel security program, which includes a standardized security approval process for extreme risk travel, as well as automated travel advisories. Global Security provides 24x7 worldwide support for the Microsoft traveler.

If you are traveling to an International Destination, be sure to....

- Review Travel Security Advisories:
<https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Services-TravelSafety-Advisory.aspx>
- Check the Country Risk list:
<https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Services-TravelSafety-CountryRisk.aspx>
- Review Security's Travel Guidelines especially if traveling to High or Extreme risk

locations:

<https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Services-TravelSafety-CountryRisk-TravelRiskGuidelines.aspx>

- Update your Contact Information (<https://hrprofile.microsoft.com>) and update also in the MS Travel online booking tool
- Confirm your access, or request access to your destinations Microsoft Facilities: <https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Services-GSAM.aspx>
- Review Business Travel Tips: <https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Services-TravelSafety-BusinessTravel.aspx>
- Review guidelines on Protecting Microsoft Intellectual Property while traveling: <https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Services-TravelSafety-ProtectingMicrosoftIP.aspx>

Look into known potential health risks present in the country of origin or destination.

- OSAC Traveling with Mobile Devices; Trends and Best Practices: <https://microsoft.sharepoint.com/sites/globalsecurity/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2Fglobalsecurity%2FShared%20Documents%2FTraveling%20with%20Mobile%20Devices%2Epdf&parent=%2Fsites%2Fglobalsecurity%2FShared%20Documents>

Know Your Destination

If you have booked travel to moderate, high or extreme risk countries, you will receive a travel advisory that you must review. For more information, contact your regional security manager.

- If you are traveling to an extreme risk destination, you must obtain approval from your manager and VP.
- After you have received your manager and VP approval, it is your responsibility to inform the Regional Security Manager of the intention to travel to an extreme risk destination.
- Do not travel to embargoed countries. For case by case exception, visit the Process for Approval of Request of Exemptions to Travel Policy for Cuba and Iran.

How to Book Travel Reservations

You must book, purchase, change, and cancel all business-related travel reservations through the designated travel agency and/or online booking tool in your country.

More Company Travel Policy available at:

<https://aka.ms/travelpolicy>

Social Engineering

Social Engineering involves the clever manipulation of the natural human tendencies of trust in order to obtain information to help facilitate fraud, network intrusion, industrial espionage and identity theft, or network/system disruption. The effort to deceive often begins with extensive background work. The social engineer may eavesdrop on conversations in common areas such as cafes, hallways, restrooms, or other public settings, or may engage in seemingly idle, innocent conversations - all in preparation for a Social Engineering attempt.

The social engineer may employ a number of strategies to gain access to information. Here are some prevention tips:

Prevent social engineering with Information Security

- Cyber criminals often use social engineering methods to obtain information that helps facilitate fraud, network intrusion, system disruption, or identity theft. Learn more about how to protect to your data, identity, and devices on [MSProtect](#).

Prevent social engineering with Physical Security

- Wear your card key in full view. If we all wear our badges, those who don't belong will be more easily identified.
- Never loan keys or access card keys.
- Never prop open entry/exit or lab doors. It could take less than a minute for someone to enter your workspace, take something, and leave the building.
- Follow Visitor Procedures. If we all comply, those who don't belong will stand out.
- Be cautious of visitors. Knowingly or unknowingly, they may observe or overhear sensitive information.
- Discourage tailgating. It's the number 1 way to gain unauthorized access.
- Follow a Clean Desk policy, and keep your desk clutter free. Your work space will be less appealing to an intruder, and if anything is missing it will be more obvious.
- Shut and lock doors (if applicable) when leaving for an extended period of time.
- Be more aware after hours and on weekends. Most people work during weekdays.

Respond to a Social Engineering Attack

Report any suspicions or concerns immediately via [Report It Now](#) (<https://reportitnow.microsoft.com/>) and/or call the Virtual Security Operations Center (VSOC).

More social engineering prevention tips available at

<https://microsoft.sharepoint.com/sites/globalsecurity/SitePages/Awareness-TheftPrevention-SocialEngineering.aspx>

Global Security Contacts

Report a Security Incident or Issue:

- Virtual Security Operations Center (VSOC) phone: +1 425 706 0000 (call for immediate response 24/7)
- WEB: <https://aka.ms/ReportItNow> or email: security@microsoft.com (response within 72 hours)

China Security On-site Contacts:

- Beijing West: +86 10 5916 9999
- Shanghai Zizhu: +86 21 61883110
- Shanghai Huaxin: +86 21 6188 9217
- Wuxi CSS: +86 510 66658910
- Suzhou Campus: +86 512 8990 8999

More security policy and advice at Global Security Website:

<https://microsoft.sharepoint.com/sites/globalsecurity>

XI. OTHERS

Useful Website Links

<http://msw> MS Internal Website

<http://hrweb> HR Website

<http://learningcentral> GCR Training

<http://idweb> Add you to the related group alias

[SuccessFactors: Home \(sapsf.com\)](#) To view personal information and modify personal information in EC.

<http://msvacation> Apply for leave and vacation (Only applicable to FTE)

<http://mspolicy/Pages/default.aspx> Microsoft Policy Website

<https://expense.microsoft.com/#> Reimbursement (Applicable to the most of FTE)

<http://myorder> Purchasing Website

<https://microsoft.sharepoint.com/teams/prclcaweb/Pages/Home.aspx> Microsoft China Law & Corporate Affairs

**Attachment --- Receipt signed by the Microsoft China employee
acknowledging that he/she has read the Employee Handbook**

Microsoft Standards of Business Conduct

Great People with Great Values
Microsoft Values
Why Microsoft Has Standards of Business Conduct
How to Use the Standards of Business Conduct
Compliance with the Standards of Business Conduct
Microsoft's Standards of Business Conduct
Microsoft's Business Conduct and Compliance Program

I am aware of the above

Signature:

Microsoft Office Guidelines

General Company Guidelines
Disciplinary Rules on Violations of Company Policies & Labor Discipline
Information Technology Guideline and Policy
Confidential I/Proprietary Information or Trade Secret
How Should I Protect Microsoft's Property – Intellectual Property
Open Source Software
Proper Use Of Microsoft and Third Party Copyrighted Materials
Anti-piracy Policy
Anti-Harassment and Anti-Discrimination
Company Access and Monitoring Information and Property
Conflict Of Interest
Rules for the Use Of E-mail and the Internet
Employee's Personal Information Processing Policy of Microsoft China

I am aware of the above

Signature:

Microsoft China Human Resources Information

Compensation Philosophy
Payroll Information
Stock Award and Employee Stock Purchase Plan
Social Benefit and Employee Benefits
MS Vacation User Guidance
How to submit leave supporting document(s)
Manage Your Personal Data
Performance and Development
Inbound / Work Permit / Residence Permit Assistance for Foreign Passport Holders
Other Information

I am aware of the above

Signature:

Microsoft China Employee Business Travel Policy and Guideline

Explore MSTravel
Company Travel Policy & Guidance
China Available information

I am aware of the above

Signature:

Microsoft China Employee Business Expense Reimbursement

Meal and Entertainment
Employee Personal Vacation
Telephone Charges
Travel Insurance

Miscellaneous
Reimbursement Procedure
Notes of Reimbursement

I am aware of the above

Signature:

Microsoft Real Estate & Facilities Services

Main Reception
Employee Meal Service
Office Equipment
Stationary Service and Business Card
Mail Service
Office Space Management
In-Office Move Service
Pantry Services
Incident Reporting
Facility Management Service Information
RE&F Global Facilities Service Center Hotline

I am aware of the above

Signature:

Microsoft Digital (formerly Microsoft IT) Handbook

Microsoft Digital Service
System Initial Settings
About Microsoft Network Environment
Microsoft Information Services General Use Standard
Related Web Sites and Software Installation

I am aware of the above

Signature:

Microsoft Global Security Instruction

Access Control
Visitor Management Procedure
Theft Prevention
Personal Safety
Emergency Preparedness
Travel Safety
Social Engineering
Global Security Contacts

I am aware of the above

Signature:

Others

Useful Website Links

I am aware of the above

Signature:

Reading instructions:

This handbook is provided for full time employees (FTE) of Microsoft China. Microsoft's continuing growth and advancement require that its benefits and policy systems change in line with this. Microsoft has the right to make the corresponding revisions to this Employee Handbook from time to time in accordance with changes in Chinese laws or changes in Company benefits, policies or Company rules governing internal production and management. Microsoft will notify by announcement on the intranet or by e-mail, its employees of the relevant changes, explain the details of such relevant changes and state the effective date of the new policy. The employee acknowledges and agrees that he/she is also obligated at all times to check the various relevant web sites of the Company to understand and comply with its latest policy and rules.

I am aware of the above

Signature:

Employee's name (print):_____

Execution date:_____