Revision History

Version	Date	Author	Major Changes
1.0	01/06/2019	Dushyant Gohil	Initial Version
1.1	15/04/2021	Dushyant Gohil	Updated document with: - Usage of Printer - Hardware Damage Expenses
1.2	23/09/2021	Kruti Shah	Lost IT Asset
1.3	10/10/2022	Kruti Shah	Update in Hardware Damage Expenses
1.4	01/12/2022	Kruti Shah	Update in Hardware Damage Expenses

INDEX

1. Email and Instant Messaging

1.1 Objective:

Provide appropriate guidelines for productively utilizing the company's email system and instant messaging technology that protects the employee and company while benefiting our business.

1.2 Applies to:

All Trainee/Interns, Employees and Consultants

1.3 Key guidelines:

- The company has established this policy about the acceptable use of company provided electronic messaging systems, including but not limited to email and instant messaging.
- Email and instant messaging are important and sensitive business tools. This policy applies to all electronic messages composed, sent, or received by any employee or by any person using company provided electronic messaging resources.
- The company sets forth the following policies but reserves the right to modify them at any time to support our company:

1.4 General:

- The company provides electronic messaging resources to assist in conducting company business.
- All messages composed and/or sent using company provided electronic messaging resources must comply with company policies regarding acceptable communication.
- The company prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources to discriminate for any or all these reasons is prohibited.
- Upon termination or separation from the company, the company will deny all access to electronic messaging resources, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.
- Each employee will be assigned a unique email address that is to be used while conducting company business via email.
- Employees are prohibited from forwarding electronic messages sent through company provided systems to external messaging systems or for any personal purpose on Job/Commercial sites.

- Employees authorized to use instant messaging programs will be advised specifically on which instant message program(s) are permissible.
- Employees authorized to use instant messaging programs will be assigned a unique instant messaging identifier, also known as a buddy name, handle or nickname.
- Electronic messages are frequently inadequate in conveying mood and context. Carefully consider how the recipient might interpret a message before composing or sending it.
- Any employee who discovers a violation of these policies should immediately notify a manager or the Human Resources Department.
- Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to, termination.

1.5 Ownership:

- The email/electronic messaging systems are company property. All messages stored in company provided electronic messaging system(s) or composed, sent, or received by any employee or non-employee are the property of the company. Electronic messages are NOT the property of any employee.
- The company reserves the right to intercept, monitor, review and/or disclose all messages composed, sent, or received.
- The company reserves the right to alter, modify, re-route, or block the delivery of messages as appropriate.
- The unique email addresses and/or instant messaging identifiers assigned to an employee are the property of the company. Employees may use these identifiers only while employed by the company.

1.6 Confidentiality

- Messages sent electronically can be intercepted inside or outside the company and as such there should never be an expectation of confidentiality. Do not disclose proprietary or confidential information through email or instant messages.
- Electronic messages can never be unconditionally and unequivocally deleted. The remote possibility of discovery always exists. Use caution and judgment in determining whether a message should be delivered electronically versus in person.
- Electronic messages are legally discoverable and permissible as evidence in a court of law. Messages should not be composed that you would not want to read out loud in a court of law.
- Employees are prohibited from unauthorized transmission of company trade secrets, confidential information, or privileged communications.

- Unauthorized copying and distribution of copyrighted materials is prohibited.

1.7 Security:

- The company employs sophisticated anti-virus software. Employees are prohibited from disabling anti-virus software running on company provided computer equipment.
- Although the company employs anti-virus software, some virus infected messages can enter the company's messaging systems. Viruses, "worms" and other malicious code can spread quickly if appropriate precautions are not taken. Follow the precautions discussed below:
    - Be suspicious of messages sent by people not known by you.
    - Do not open attachments unless they were anticipated by you. If you are not sure, always verify the sender is someone you know and that he or she sent you the email attachment.
    - Disable features in electronic messaging programs that automatically preview messages before opening them.
    - Do not forward chain letters. Simply delete them.
- The company considers unsolicited commercial email (spam) a nuisance and a potential security threat. Do not attempt to remove yourself from future delivery of a message that you determine is spam. These "Remove Me" links are often used to verify that you exist.
- Internet message boards are a fertile source from which mass junk e-mailers harvest email addresses and email domains. Do not use company provided email addresses when posting to message boards.

1.8 Inappropriate use:

- Email or electronic messaging systems may not be used for transmitting messages containing pornography, profanity, derogatory, defamatory, sexual, racist, harassing, or offensive material.
- Company provided electronic messaging resources may not be used for the promotion or publication of one's political or religious views, the operation of a business or for any undertaking for personal gain.

Tools to be used For E-mail and Instant Messaging are Office365 and Microsoft Teams.

2. Internet usage:

2.1 Objective:

Provide appropriate guidelines for accessing and utilizing the Internet through the company's network.

2.2 Applies to:

All Trainee/Interns, Employees and Consultants with authorized access to Internet services.

2.3 Key guidelines:

Internet services are authorized to designated employees by their manager to enhance their job responsibility. The Internet is an excellent tool but also creates security implications that the company must guard against. For that reason, employees are granted access only as a means of providing support in fulfilling their job responsibility.

2.4 General:

- Internet accounts are approved for designated employees by their immediate manager to provide tools that assist in their work.
- Everyone is responsible for the account issued to him/her.
- Sharing Internet accounts or User-ID's is prohibited.
- Organizational use of Internet services must reflect the mission of the company and support the company's goals and objectives.
- These services must support legitimate, mission related activities of the company and be consistent with prudent operational, security, and privacy considerations.
- The CIO led Internet Steering Committee will take responsibility for all web site content (i.e., "the company web site") and format presentation to reflect the company's mission and in supporting company and departmental objectives.
- The Company has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
- Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

2.5 Inappropriate use:

- The following uses of company provided Internet access are not permitted:
    - To access, upload, download, or distribute pornographic or sexually explicit material.
    - Violate and state, local, or federal law.
    - Vandalize or damage the property of any other individual or organization.
    - To invade or abuse the privacy of others.
    - Violate copyright or use intellectual material without permission.
    - To use the network for financial or commercial gain
    - To degrade or disrupt network performance.
- No employee may use company facilities knowingly to download or distribute pirated software or data. The use of file swapping software on company computers and company networks is prohibited.
- No employee may use the company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

Note: All activities which happen over network/Internet are logged.

3. Password security

3.1 Objective:

Provide guidelines in appropriate management of business passwords to maintain adequate security and integrity of all the company's business systems.

3.2 Applies to:

All Trainee/Interns, Employees and Consultants

3.3 Key guidelines:

Maintaining security of the company's business applications, software tools, email systems, network facilities, and voice mail are critical to providing data integrity and stability of our systems. Passwords are provided to limit access to these company assets on an as needed basis.

- The company provides access to network, electronic mail, and voice mail resources to its employees in support of the company's mission. Passwords are assigned for access

to each of these resources to authenticate a user's identity, to protect network users, and to provide security.

- It is the responsibility of everyone to protect and to keep private any and all passwords issued to him/her by the company.
- The IT Department will establish guidelines for issuing new passwords, deleting passwords as required, and allowing employees to change their passwords.
- Although the company strives to manage a secure computing and networking environment, the company cannot guarantee the confidentiality or security of network, e- mail, or voice mail passwords from unauthorized disclosure.
- New employee passwords and changes must be requested by a manager. This helps monitor and manage the importance of protecting passwords in their distribution and use in such a way that reinforces the integrity of users accessing company systems.
- A network manager must approve any password change requested by a user's supervisor. Confirmation will be sent to user when a password change is completed at the request of a supervisor.
- IT Customer Support will handle requests from company managers made in one of the following ways:
    - Requests may be made in person from 10:00am to 5:00pm Monday-Friday.
    - Requests may be submitted via Ticketing System.
    - Password account requests must be verified by the employee's manager.
- The IT Department will delete all passwords of exiting employees upon notification from Human Resources.
    - System administrators and employees assume the following responsibilities:
    - System administrator must protect confidentiality of user’s password.
    - Employees must manage passwords according to the Password Guidelines.
    - Employee is responsible for all actions and functions performed by his/her account.
    - Suspected password compromise must be reported to IT Support immediately.

3.4 Password Guidelines:

Select a Wise Password

To minimize password guessing:

- Do not use any part of the account identifier (username, login ID, etc.).
- Use 8 or more characters.
- Use mixed alpha, numeric and special characters.
- Use two or three short words that are unrelated.

Keep Your Password Safe

- Do not tell your password to anyone.
- Do not let anyone observe you entering your password.
- Do not display your password in your work area or any other highly visible place.
- Change your password periodically (every 3 months is recommended).
- Do not reuse old passwords.

Additional Security Practices

- Ensure your system/laptop is reasonably secure in your absence from your office. Consider using a password-protected screen saver, lock, logging off or turning off your system/laptop when you leave your desk.

4. Software usage:

4.1 Objective:

Provide guidelines on appropriate use of software products utilizing company equipment.

4.2 Applies to:

All Trainee/Interns, Employees and Consultants

4.3 Key guidelines:

This policy is intended to ensure that all company employees understand that no computer software may be loaded onto or used on any computer owned or leased by the company unless the software is the property of or has been licensed by the company.

4.4 General:

- Software purchased by the company or residing on company owned computers is to be used only within the terms of the license agreement for that software title.
- Unless otherwise specifically provided for in the license agreement, any duplication of copyrighted software, except for archival purposes is a violation of copyright law and contrary to the company's Software Usage Policy.
- To purchase software, employees must obtain the approval of their department manager who will follow the same procedures used for acquiring other company assets.
- All approved software will be purchased through the Purchasing Department.

- The CIO and designated members of the IT Department will be the sole governing body for defining appropriate software titles acceptable for use in the company.
- Under no circumstances will third party software applications be loaded onto company owned computer systems without the knowledge of and approval of the IT Department.
- Illegal reproduction of software is subject to civil and criminal penalties, including fines and imprisonment. Any company user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances and may include termination of employment.
- The company does not condone the illegal duplication of software in any form.

4.5 Compliance:

- We will use all software in accordance with its license agreements.
- Under no circumstances will software be used on company computing resources except as permitted in the company's Software Usage Policy.
- Legitimate software will be provided to all employees who need it. Company employees will not make unauthorized copies of software under any circumstances. Anyone found copying software other than for backup purposes is subject to termination.
- Each Employee of software purchased and licensed by the company must acquire and use that software only in accordance with the company's Software Usage Policy and the applicable Software License Agreement.
- All Employees acknowledge that software and its documentation are not owned by the company or an individual but licensed from the software publisher.
- Employees of the company are prohibited from giving company acquired software to anyone who does not have a valid software license for that software title. This shall include but is not limited to clients, vendors, colleagues, and fellow employees.
- All software used by a company entity for company owned computing devices, or purchased with company funds, will be acquired through the appropriate procedures as stated in the company Software Usage Policy.
- Any employee who determines that there may be a misuse of software within the organization will notify the software manager or department manager.

4.6 Registration of software:

- Software licensed by the company will not be registered in the name of an individual.
- When software is delivered, it must first be properly registered with the software publisher via procedures appropriate to that publisher. Software must be registered in the name of the company with the job title or department name in which it is used.
- After the registration requirements above have been met, the software may be installed in accordance with the policies and procedures of the company. A copy of the license agreement will be filed and maintained by the IT Department's Software License Administrator.
- Once installed, the original installation media should be kept in a safe storage area designated by the IT Department.
- Shareware software is copyrighted software that is distributed freely through bulletin boards, online services, and the Internet. The company's policy is to pay shareware authors the fee they specify for use of their products if the software will be used at the company. Installation and registration of shareware products will be handled the same way as for commercial software products.

4.7 Software Audit:

- IT Team will conduct periodic audits of all company owned PCs, including laptops, to ensure the company is in compliance with all software licenses.
- Audits will be conducted using an auditing software product.
- Software for which there is no supporting registration, license, and/or original installation media will be removed immediately from the employee's computer.
- During these audits, the software manager will search for computer viruses and eliminate any that are found.
- The full cooperation of all employees is required during software audits.

5. PC software standards:

5.1 Objective:

Provide guidelines for purchasing and installing software on company PC’s.

5.2 Applies to:

All Trainee/Interns, Employees and Consultants

5.3 Key guidelines:

The purpose for this policy is to explain company software standards and to identify the levels of technical support available to the company employees from the IT Department.

5.4 Applicability:

- This policy applies to All Trainee/Interns, Employees and Consultants of the company requesting the purchase of new computer software and who desire computing support for that application from the IT technical support team.
- The following software standards have been established to ensure efficient and cost-effective use of company computing assets:
  - To help ensure compatibility between applications and releases.
  - To provide more effective system administration
  - To assist in the computer planning process and enable the realization of long-term goals and the future computing vision.
  - To ensure cost effective purchasing
  - To enable effective tracking of software licenses
  - To provide cost effective end user software training
  - To facilitate efficient and effective technical support effort

5.5 Technical Support:

- Software support is provided at several levels and is based on whether the software is the company enterprise standard or department specific.
- The IT Department will not provide support for evaluation software, personally purchased software, illegal copies of software, screen savers, shareware, and nonnetwork software that is not included in the standard software list.
- Software applications determined by IT technical staff to cause computer problems with the company's standard network software will be removed.

5.6 IT Department's Role in The Purchase of Hardware and Software:

- Assist departments with evaluating new business software solution.
- Act as liaison for departments when dealing with computing vendors.
- Recommend and evaluate the tasks/jobs/functions to be accomplished via the new software product.
- Assist with hardware and system requirements.
- Install the software as needed.
- Enforce company hardware and software standards.

5.7 Standard PC Equipment and Software List:

- Standard PC hardware and software configurations are posted on the company's Portal in the IT Department section.
- Contact the Systems Support Manager of the IT Department for questions pertaining to company standards.

5.8 Requesting Standard PC Equipment and Software:

- Equipment and software requests that are covered by the company's PC Equipment and Software Standards List will be provided quickly if appropriate approvals are granted.
- The steps that follow outlines the process for purchasing PC equipment and software:
  - Complete the PC Equipment and Software Request from AMS (Asset Management System).
  - Gain approval of the Department Manager
  - Submit request to IT Department's System Support Manager.
  - The IT Department will review the order and forward to Purchasing or will contact Requester for clarification as needed.
  - The IT Department or Purchasing Department are available for follow-up questions regarding your order as needed.

5.9 Request for a Variance from the PC Hardware or Software Standard:

- complete the "Request for a Variance from the PC Hardware and Software Standard" using AMS.
- Practical and sufficient justification is a key part so be concise in building your case for deviating from the standard.
- Gain approval of the request from your Department Manager.
- Submit the request to the IT Department's Systems Support Manager for review.
- Your request is reviewed and either approved or declined based upon justified reasons presented and the IT Department's ability to support the new configuration within the company's network.

6. Remote access:

6.1 Objective:

Provide guidelines on appropriate use of remote access capabilities to the company's network, business applications, and systems.

6.2 Applies to:

All Trainee/Interns, Employees and Consultants

6.3 Key guidelines:

- The purpose of this policy is to define standards for connecting to the company network from a remote location outside the company.
- These standards are designed to minimize the potential exposure to the company from damages that may result from unauthorized use of the company resources. Damages include the loss of sensitive or confidential company data, intellectual property, damage to critical company internal systems, etc.
- This policy applies to all the company employees, contractors, vendors, and agents with a company owned or personally owned computer or workstation used to connect to the company network.
- This policy applies to remote access connections used to do work on behalf of the company, including reading or sending email and viewing Intranet web resources.
- Remote access implementations that are covered by this policy include, but are not limited to, Routers, VPN, SSH, FTP, System/Laptops etc.
- It is the responsibility of the company employees, contractors, vendors, and agents with remote access privileges to the company's corporate network to ensure that their remote access connection is given the same consideration as the employee's on-site connection to the company network.

6.4 Remote connection:

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password phrases.
- At no time should any company employee provide his/her login or email password to anyone, not even family members.
- Company employees and contractors with remote access privileges must ensure that their company owned or personal computer or workstation, which is remotely connected to the company's corporate network, is not connected to any other network at the same time.

- The company employees and contractors with remote access privileges to the company's corporate network must not use noncompany email accounts (i.e. Yahoo, AOL), or other external resources to conduct the company business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the company network must meet minimum authentication requirements established by the IT Department.
- All hosts that are connected to the company internal networks via remote access technologies must use the most up-to-date anti-virus software.
- Third party connections must comply with requirements defined by the IT Department.
- Personal equipment that is used to connect to the company's networks must meet the requirements of the company-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the company production network must obtain prior approval from the IT Department.

6.5 Enforcement:

- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
- The IT Department is responsible for monitoring remote access and addressing inappropriate use of remote access privileges.

7. Printer Usage:

7.1 Objective:

Provide guidelines, how you can use printer of company.

7.2 Applies to:

All Trainee/Interns, Employees and Consultants

7.3 Key guidelines:

- One can get printer installed by help of IT Team by raising a support ticket over helpdesk portal.
- Any Trainee/Employee/Consultant can take black & white print up to 10 pages from black & white printer.
- One needs to get prior approval of their PM/TL or member of IT Team to get a color print.

8. Hardware Damage Charges:

8.1 Objective:

Provide guidelines on inappropriate use of assets (Laptop/Mouse/Headphones etc.) provided by organization (Techforce Infotech Pvt Ltd).

8.2 Applies to:

All Trainee/Interns, Employees and Consultants

8.3 Key guidelines:

- In case of **Hardware or Software failure** in any asset, IT Team will take care for the recovery or maintenance of the same.

  Though the Trainee/Interns, Employees, or Consultants are entitled to pay repair/ maintenance charges as mentioned below for such maintenance:

Damage Cost (Rs.)	Employee %	Company %
Up to 2500	100	0
2500 to 5000	85	15
5000 or more	80	20

  ** This may vary from case to case based on final review from IT Team and final decision will be taken by IT Team.

- In case of **Hardware physical damage or Liquid damage** in any asset, the repairing / maintenance will be taken care by IT team.
  All expenses (100%) for such damage/ maintenance along with the penalty up to Rs. 5000/- (minimum will be Rs 1000-) will be borne by the concern Trainee/ Employee/ Consultant.
  Final penalty charges will be based on the case. Final decision will be taken by the IT Team and Management, which one will be required to adhere to.

9. Lost IT Assets:

9.1 Objective:

Provide guidelines on lost assets (Laptop/Mouse/Headphones/Laptop Bags etc.) provided by organization (Techforce Infotech Pvt Ltd).

9.2 Applies to:

All Trainee/Interns, Employees and Consultants

9.1 Key guidelines:

- In case of loss of any IT asset which belongs to Techforce Infotech Pvt Ltd, Employee is bound to pay the amount as per following calculation in lieu of that asset.

Duration (Based on Purchase date from Invoice)	**Amount to pay (% Of Invoice Amount)**
Up to 1 Year	100%
Between 1 to 2 years	80%
Between 2 to 3 Years	64%
Between 3 to 4 Years	51%
Above 4 years	40%