A black and grey logo

Description automatically generated

Security Policy for Microsoft

By Seven Gunthrope

Contents

[A black and grey logo

Description automatically generated 3](#_Toc165296083)

[Microsoft Overview 3](#_Toc165296084)

[Abstract 4](#_Toc165296085)

[General Policies 6](#_Toc165296086)

[Password Construction Policy 6](#_Toc165296087)

[Password Protection Policy 10](#_Toc165296088)

[Ethics Policy 13](#_Toc165296089)

[Acceptable Use Policy 16](#_Toc165296090)

[Network Policies 23](#_Toc165296091)

[Router and Switch Security Policy 23](#_Toc165296092)

[Employee Internet use Monitoring and Filtering Policy 29](#_Toc165296093)

[Remote Access Policy 32](#_Toc165296094)

[Remote Access Tools Policy 35](#_Toc165296095)

[Acquisition and Merger Assessment Policy 38](#_Toc165296096)

[Server Security Policies 41](#_Toc165296097)

[Database Credentials Coding Policy 41](#_Toc165296098)

[Server Malware Protection Policy 44](#_Toc165296099)

[Server Audit Policy 47](#_Toc165296100)

[Server Security Policy 49](#_Toc165296101)

[Application Security Policies 52](#_Toc165296102)

[Software Installation Policy 52](#_Toc165296103)

[Web Application Security Application 54](#_Toc165296104)

[Definitions and Terms Page 57](#_Toc165296105)

[References 59](#_Toc165296106)

[Definition References 59](#_Toc165296107)

[Picture References 59](#_Toc165296108)

# A black and grey logo Description automatically generated

# Microsoft Overview

Microsoft is a computer technology company that is also a global vendor for the operating system that everybody in the world uses or has used today because of this they have a network infrastructure that spans across the globe and needs to be protected both physically and of course digitally. Not only that they also provide applications such as Microsoft word, excel PowerPoint etc. Lastly, they provide a cloud infrastructure or Azure which they used to access the applications, creation of virtual machines, creation of AI and its functions and due to this they need policies that will protect their employees and the end users who download their product. Which is why I am going to supply policies for each section which include General Security, Network Security, Server Security and Application security.

# Abstract

Microsoft is a global company that will need many layers of policies to not only protect their employees but their end users, networking infrastructure, applications etc. After researching it became clear that they have many aspects that need policies in four major areas general security, networking security, server security, and application security. The reason being is because they are a global company with many offices who offer their applications and services worldwide and uses them for all operations and these offices are not only restricted to on-premises, but they are also remote, hybrid offices which means all four of these topics are of the utmost importance. The reason why Microsoft would want these policies is to first protect their assets if these policies where not in effect there would be no order in how they go about safeguarding information and then in turn would just be a mystery to everyone not only that but without them employees will not care or pay attention to how they conduct business. These security policies will protect their employees and end users by instructing them on how they should go about using their applications and how they should be protecting their credentials to not allow any bad actors to mess with their work. Not only that but it gives public transparency allowing them to understand more of the security of the infrastructure they are inputting their personal information into.

# General Policies

# Password Construction Policy

1. **Overview**

Passwords are a critical component of information security. Passwords serve to protect access to user accounts, data, and systems. However, a poorly constructed or easily guessed password can compromise the strongest defenses. This guideline provides best practices for creating strong passwords.

1. **Purpose**

The purpose of these guidelines is to provide best practices for the creation of strong passwords.

1. **Scope**

This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, and local router logins.

1. **Policy**

Strong passwords are long, the more characters a password has the stronger it is. We recommend a minimum of sixteen characters in all work-related passwords. In addition, we encourage the use of passphrases, passwords made up of multiple words. Examples include “*It’s time for vacation*” or “*block-curious-sunny-leaves*.” Passphrases are both easy to remember and type yet meet the strength requirements.

Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change.

1. **Policy Compliance**
   1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to password cracking exercises, business tool reports, internal and external audits, and feedback to the policy owner.

* 1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

* 1. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Password Protection Policy

Overview

Passwords are a critical aspect of computer security. A weak or compromised password can result in unauthorized access to our most sensitive data and/or exploitation of our resources. All staff, including contractors and vendors with access to Microsoft systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for the secure use and protection of all work-related passwords.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Microsoft facility, has access to the Microsoft network, or stores any non-public Microsoft information.

Policy

Password Creation and Use

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own personal accounts.

4.1.3 Staff are allowed to use authorized, approved password managers to securely store and manage all their work-related passwords.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

Password Change

Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet our Password Creation Requirements. We do not recommend the use or setting of regular password expiration unless the user is a part of multiple high-level projects.

Password Protection

Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, Confidential Microsoft information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

Passwords may be stored only in password managers authorized by the organization.

Do not use the "Remember Password" feature of applications (for example, web browsers).

Any individual suspecting that their password may have been compromised must report the incident and change all relevant passwords.

Application Development

Application developers must ensure that their programs contain the following security precautions:

Applications must support authentication of individual users, not groups.

Applications must not store passwords in clear text or in any easily reversible form.

Applications must not transmit passwords in clear text over the network.

Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Multi-Factor Authentication

Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

• Password Construction Guidelines

# Ethics Policy

Overview

Microsoft is committed to protecting employees, partners, vendors, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Microsoft addresses issues proactively and uses correct judgment, it will help set us apart from competitors.  
  
Microsoft will not tolerate any wrongdoing or impropriety at any time. Microsoft will take the appropriate measures and act quickly in correcting the issue if the ethical code is broken.

Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee’s and consumer’s expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every Microsoft employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

Scope

This policy applies to employees, contractors, consultants, temporary workers, and other workers at Microsoft, including all personnel affiliated with third parties.

Policy

Executive Commitment to Ethics

Senior leaders and executives within Microsoft must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

Executives must have an open-door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

Executives must disclose any conflict of interest regarding their position within Microsoft.

Employee Commitment to Ethics

Microsoft employees will treat everyone fairly, have mutual respect, promote a team environment, and avoid the intent and appearance of unethical or compromising practices.

Every employee needs to apply effort and intelligence in maintaining ethical value.

Employees must disclose any conflict of interest regarding their position within Microsoft.

Employees will help Microsoft to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

Employees should consider the following questions to themselves when any behavior is questionable:

Is the behavior legal?

Does the behavior comply with all appropriate Microsoft policies?

Does the behavior reflect Microsoft values and culture?

Could the behavior adversely affect company stakeholders?

Would you feel personally concerned if the behavior appeared in a news headline?

Could the behavior adversely affect Microsoft if all employees, did it?

Company Awareness

Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

Microsoft will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

Maintaining Ethical Practices

Microsoft will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs to consistently maintain an ethical stance and support ethical behavior.

Employees at Microsoft should encourage open dialogue, get honest feedback, and treat everyone fairly, with honesty and objectivity.

Microsoft has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

Employees are required to recertify their compliance with the Ethics Policy on an annual basis.

Unethical Behavior

Microsoft will avoid the intent and appearance of unethical or compromising practice in relationships, actions, and communications.

Microsoft will not tolerate harassment or discrimination.

Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

Microsoft will not permit impropriety at any time, and we will act ethically and responsibly in accordance with laws.

Microsoft employees will not use corporate assets or business relationships for personal use or gain.

Policy Compliance

Compliance Measurement

The Microsoft legal/Ethics Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

Exceptions

None.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Acceptable Use Policy

Overview

Infosec Team’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Microsoft’s established culture of openness, trust, and integrity. Microsoft is committed to protecting Microsoft's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Microsoft. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Microsoft employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and other electronic devices at Microsoft. These rules are in place to protect the employees and Microsoft. Inappropriate use exposes Microsoft to cyber risks including virus attacks including ransomware, compromise of network systems and services, data breach, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Microsoft business or interact with internal networks and business systems, whether owned or leased by Microsoft, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Microsoft and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Microsoft policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to employees, contractors, consultants, temporary workers, and other workers at Microsoft, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Microsoft.

Policy

General Use and Ownership

Microsoft proprietary information stored on electronic and computing devices whether owned or leased by Microsoft, the employee or a third party, remains the sole property of Microsoft. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Microsoft proprietary information.

You may access, use, or share Microsoft proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of the Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

For security and network maintenance purposes, authorized individuals within Microsoft may monitor equipment, systems, and network traffic at any time, per Infosec's *Audit Policy*.

Microsoft reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

**Security and Proprietary Information**

All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected lock screen with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Postings by employees from a Microsoft email address to newsgroups or other online platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Microsoft, unless posting is during business duties.

Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

**Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Microsoft authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Microsoft-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

**System and Network Activities**

The following activities are prohibited, with no exceptions:

Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Microsoft.

Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Microsoft or the end user does not have an active license is prohibited.

Accessing data, a server, or an account for any purpose other than conducting Microsoft business, even if you have authorized access, is prohibited.

Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.

Introduction of malicious programs into the network or server (e.g., viruses, worms, trojan horses, ransomware, etc.).

Revealing your account password/passphrase to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Using a Microsoft computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

Making fraudulent offers of products, items, or services originating from any Microsoft account.

Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, brute-forcing accounts, and forged routing information for malicious purposes.

Port scanning or security scanning is expressly prohibited unless prior notification to the Infosec Team is made.

Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.

Circumventing user authentication or security of any host, network, or account.

Introducing honeypots, honeynets, or similar technology on the Microsoft network.

Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Providing information about, or lists of, Microsoft employees to parties outside Microsoft.

**Email and Communication Activities**

When using company resources to access and use the Internet, users must realize theyrepresent the company. Whenever employees state an affiliation with the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

Any form of harassment via email, telephone, text, or paging, whether through language, frequency, or size of messages.

Unauthorized use, or forging, of email header information.

Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Use of unsolicited email originating from within Microsoft's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Microsoft or connected via Microsoft's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**Blogging and Social Media**

Blogging or posting to social media platforms by employees, whether using Microsoft’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Microsoft’s systems to engage in blogging or other online posting is acceptable, if it is done in a professional and responsible manner, does not otherwise violate Microsoft’s policy, is not detrimental to Microsoft’s best interests, and does not interfere with an employee's regular work duties. Blogging or other online posting from Microsoft’s systems is also subject to monitoring.

Microsoft’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Microsoft confidential or proprietary information, trade secrets or any other material covered by Microsoft’s Confidential Information policy when engaged in blogging.

Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Microsoft and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Microsoft’s *Non-Discrimination and Anti-Harassment* policy.

Employees may also not attribute personal statements, opinions or beliefs to Microsoft when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee or representative of Microsoft. Employees assume all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Microsoft’s trademarks, logos, and any other Microsoft intellectual property may also not be used in connection with any blogging or social media activity.

Policy Compliance

Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

Data Classification Policy

Data Protection Standard

Social Media Policy

Minimum Access Policy

Password Policy

Definitions and Terms

The following definition and terms can be found on the Definitions page.

* Blogging
* Honeypot
* Honeynet
* Proprietary Information
* Spam
* Ransomware

# Network Policies

# Router and Switch Security Policy

Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of Microsoft.

Scope

All employees, contractors, consultants, temporary and other workers at Microsoft and its subsidiaries must adhere to this policy. All routers and switches connected to Microsoft production networks are affected.

Policy

Every router must meet the following configuration standards:

No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentications.

The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device’s support organization.

The following services or features must be disabled:

IP directed broadcasts.

Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses.

TCP small services

UDP small services

All source routing and switching.

All web services run on a router.

Microsoft discovery protocol on Internet connected interfaces

Telnet, FTP, and HTTP services

Auto-configuration

The following services should be disabled unless a business justification is provided:

Microsoft discovery protocol and other discovery protocols

Dynamic trunking

Scripting environments, such as the TCL shell

The following services must be configured:

Password-encryption

NTP configured to a corporate standard source.

All routing updates shall be done using secure routing updates.

Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

Access control lists for transiting the device are to be added as business needs arise.

The router must be included in the corporate enterprise management system with a designated point of contact.

Each router must have the following statement presented for all forms of login whether remote or local:

*"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."*

Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

IP access list accounting

Device logging

Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped.

Router console and modem access must be restricted by additional security controls.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Overview

Remote access to our corporate network is essential to maintain our Team’s productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks to the best of our ability.

Purpose

The purpose of this policy is to define rules and requirements for connecting to Microsoft's network from any host. These rules and requirements are designed to minimize the potential exposure to Microsoft from damages which may result from unauthorized use of Microsoft resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Microsoft internal systems, and fines or other financial liabilities incurred because of those losses.

Scope

This policy applies to all Microsoft employees, contractors, vendors, and agents with a Microsoft-owned or personally owned computer or workstation used to connect to the Microsoft network. This policy applies to remote access connections used to do work on behalf of Microsoft, including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to Microsoft networks.

Policy

It is the responsibility of Microsoft employees, contractors, vendors, and agents with remote access privileges to Microsoft's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Microsoft.

General access to the Internet for recreational use through the Microsoft network is limited to Microsoft employees, contractors, vendors, and agents (hereafter referred to as “Authorized Users”). When accessing the Microsoft network from a personal computer, Authorized Users are responsible for preventing access to any Microsoft computer resources or data by non-Authorized Users. Performance of illegal activities through the Microsoft network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Microsoft networks to access the Internet for outside business interests.

For additional information regarding Microsoft's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website Microsoft.com.

Requirements

Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.

Authorized Users shall protect their login and password, even from family members.

While using a Microsoft-owned computer to remotely connect to Microsoft's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

Use of external resources to conduct Microsoft business must be approved in advance by InfoSec and the appropriate business unit manager.

All hosts that are connected to Microsoft internal networks via remote access technologies must use the most up-to-date anti-virus software Microsoft.com, this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.

Personal equipment used to connect to Microsoft's networks must meet the requirements of Microsoft-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to Microsoft Networks*.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Microsoft’s network:

* *Acceptable Encryption Policy*
* *Acceptable Use Policy*
* *Password Policy*

# Employee Internet use Monitoring and Filtering Policy

Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within Microsoft's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner and ensure that employee web use can be monitored or researched during an incident.

Scope

This policy applies to all Microsoft employees, contractors, vendors, and agents with a Microsoft-owned or personally owned computer or workstation connected to the Microsoft network.

This policy applies to all end user-initiated communications between Microsoft’s network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

Policy

4.1 Web Site Monitoring

The Information Technology Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

4.2 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to any employee as needed upon request to the Information Technology Department. Computer Security Incident Response Team (CSIRT) members may access all reports and data if necessary to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to associates outside the CSIRT upon written or email request to Information Systems from a Human Resources Representative.

3.3 Internet Use Filtering System

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for Microsoft’s corporate environment. The following protocols and categories of websites should be blocked:

Adult/Sexually Explicit Material

Advertisements & Pop-Ups

Chat and Instant Messaging

Gambling

Hacking

Illegal Drugs

Intimate Apparel and Swimwear

Peer to Peer File Sharing

Personals and Dating

Social Network Services

SPAM, Phishing and Fraud

Spyware

Tasteless and Offensive Content

Violence, Intolerance and Hate

Web Based Email

3.4 Internet Use Filtering Rule Changes

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. Human Resources shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

3.5 Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a ticket to the Information Technology help desk. An IT employee will review the request and un-block the site if it is mis-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Human Resources representative. HR will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None.

Definitions and Terms

The following definition and terms can be found on the Definitions and Terms page.

* Peer to Peer File Sharing
* Social Networking Services
* SPAM
* Phishing
* Hacking

# Remote Access Policy

Overview

Remote access to our corporate network is essential to maintain our Team’s productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks to the best of our ability.

Purpose

The purpose of this policy is to define rules and requirements for connecting to Microsoft's network from any host. These rules and requirements are designed to minimize the potential exposure to Microsoft from damages which may result from unauthorized use of Microsoft resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Microsoft internal systems, and fines or other financial liabilities incurred because of those losses.

Scope

This policy applies to all Microsoft employees, contractors, vendors, and agents with a Microsoft-owned or personally owned computer or workstation used to connect to the Microsoft network. This policy applies to remote access connections used to do work on behalf of Microsoft, including reading or sending email and viewing intranet web resources. This policy covers all technical implementations of remote access used to connect to Microsoft networks.

Policy

It is the responsibility of Microsoft employees, contractors, vendors, and agents with remote access privileges to Microsoft's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Microsoft.

General access to the Internet for recreational use through the Microsoft network is limited to Microsoft employees, contractors, vendors, and agents (hereafter referred to as “Authorized Users”). When accessing the Microsoft network from a personal computer, Authorized Users are responsible for preventing access to any Microsoft computer resources or data by non-Authorized Users. Performance of illegal activities through the Microsoft network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User’s access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Microsoft networks to access the Internet for outside business interests.

For additional information regarding Microsoft's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website Microsoft.com.

Requirements

Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.

Authorized Users shall protect their login and password, even from family members.

While using a Microsoft-owned computer to remotely connect to Microsoft's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

Use of external resources to conduct Microsoft business must be approved in advance by InfoSec and the appropriate business unit manager.

All hosts that are connected to Microsoft internal networks via remote access technologies must use the most up-to-date anti-virus Microsoft.com, this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.

Personal equipment used to connect to Microsoft's networks must meet the requirements of Microsoft-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to Microsoft Networks*.

Policy Compliance

Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Microsoft’s network:

* *Acceptable Encryption Policy*
* *Acceptable Use Policy*
* *Password Policy*

# Remote Access Tools Policy

Overview

Remote desktop software, also known as remote access tools, provides a way for computer users and support staff alike to share screens, access work on a computer system from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, and Windows Remote Desktop (RDP). While these tools can save considerable time and money by eliminating travel and enabling collaboration, they also provide a back door into the Microsoft network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on Microsoft computer systems.

Purpose

This policy defines the requirements for remote access tools used at Microsoft.

Scope

This policy applies to all remote access where either end of the communication terminates at a Microsoft computer asset.

Policy

All remote access tools used to communicate between Microsoft assets and other systems must comply with the following policy requirements.

4.1 Remote Access Tools

Microsoft provides mechanisms to collaborate between internal users, with external partners, and from non-Microsoft systems. The approved software list can be obtained from https://www.microsoft.com/en-us/microsoft-365/products-apps-services. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

4.1.1 All remote access tools or systems that allow communication to Microsoft resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.

4.1.2 The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks such as OAuth 2.0. The remote access tool must mutually authenticate both ends of the session.

4.1.3 Remote access tools must support the Microsoft application layer proxy rather than direct connections through the perimeter firewall(s).

4.1.4 Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Microsoft network encryption protocols policy.

4.1.5 All Microsoft antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard Microsoft procurement process, and the information technology group must approve the purchase.

Policy Compliance

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None.

Definitions and Terms

The following definition and terms can be found on the Definitions and Terms Page

* Application layer proxy

# Acquisition and Merger Assessment Policy

Purpose

The purpose of this policy is to establish our organization’s responsibilities regarding corporate acquisitions and mergers. This policy also defines the minimum-security requirements involved in the Information Security acquisition assessment.

Scope

This policy applies to all companies acquired by Microsoft and pertains to all systems, networks, laboratories, test equipment, hardware, software, and firmware, owned and/or operated by the acquired company.

The process of integrating a newly acquired company can have a drastic impact on the security posture of either the parent company or the child company. The network and security infrastructure of both entities may vary, and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

Assess the company’s security landscape, posture, and policies.

Protect both Microsoft and the acquired company from increased security risks.

Educate acquired company’s team members about Microsoft policies and standards.

Adopt and implement Microsoft Security Policies

Integrate acquired company.

Continuous monitoring and auditing of the acquired company.

Policy Statements

General

Acquisition assessments are conducted to ensure that a company being acquired by Microsoft does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. The Information Security Team will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Information Security role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work along with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to Microsoft's networks. Below are the minimum requirements that the acquired company must meet before being connected to the Microsoft network.

Hosts

All endpoints (servers, desktops, laptops) will be replaced or re-imaged with Microsoft standard security baseline configuration and will be required to maintain this minimum standard.

Business critical production servers that cannot be replaced or re-imaged must be audited. There must be an exception granted and documented by the Information Security Team.

All end-point computing devices will require Microsoft approved anti-virus protection and/or Endpoint Detection and Response software (EDR) before network connection is established.

Networks

All network devices will be replaced or re-imaged with a Microsoft standard baseline configuration.

Wireless network access points will be configured to the Microsoft standard baseline configuration.

The acquired company’s network must comply with Microsoft network standard security baseline configuration.

Internet

All Internet connections will be terminated.

When justified by business requirements, air-gapped Internet connections will require the Information Security Team’s review and approval.

Remote Access

All remote access connections will be terminated.

Remote access to any production, test, development, or guest network will be provided by Microsoft.

Labs

Lab equipment must be physically separated and secured from non-lab areas.

The lab network must be separated from the corporate production network with a Virtual network (VLAN) with a firewall between the two networks.

Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Information Security Team or the Lab Security Group (LabSec).

All acquired labs networks must conform with the LabSec standard security baseline configuration.

In the event the acquired networks and computer systems fail to meet these requirements, the Microsoft Chief Risk Officer (CRO) must acknowledge and approve of the risk to Microsoft's networks.

Responsibility

The Chief Information Security Officer of our organization or a designee from the Governance committee will oversee and sign off on these Information Security policies. In smaller organizations, this may be the Information Security Manager. All employees, volunteers, and contractors are responsible for reading, understanding, and complying with our organization's information security policies.

Compliance and Exceptions

The Information Security Team (InfoSec Team) will verify compliance to this policy through various methods, including but not limited to, reports from business tools, external audits, internal assessments, and interaction with the policy owner.

Any exception to the policy must be approved by the Infosec team in advance.

An employee, volunteer, or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination.

# Server Security Policies

# Database Credentials Coding Policy

1. **Overview**

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of extremely sensitive assets and be a springboard to wider compromise within the organization.

1. **Purpose**

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Microsoft's networks.

Software applications running on Microsoft's networks may require access to one of the many internal database servers. To access these databases, a program must authenticate the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

1. **Scope**

This policy is directed at all system implementers and/or software engineers who may be coding applications that will access a production database server on the Microsoft Network. This policy applies to all software (programs, modules, libraries or APIS that will access a Microsoft, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they do not always use sanitized information.

1. **Policy**
   1. **General**
      1. To maintain the security of Microsoft's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text or easily reversible encryption. Database credentials must not be stored in a location that can be accessed through a web server. Algorithms in use must meet the standards defined for use in NIST publication [FIPS 140-2](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm) or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.
   2. **Specific Requirements**
      1. Storage of Data Base Usernames and Passwords
         * Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
         * Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
         * Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.
         * Database credentials may not reside in the documents tree of a web server.
         * Passwords or pass phrases used to access a database must adhere to the Password Policy.
   3. **Retrieval of Database Usernames and Passwords**
      1. If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.
      2. The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.
      3. For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.
   4. **Access to Database Usernames and Passwords**
      1. Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
      2. Database passwords used by programs are system-level passwords as defined by the Password Policy.
      3. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.
      4. Users and/or software accessing sensitive data must be subjected to proper access control and should not be able to perform privileged operations that are out of scope of said user and/or software.
   5. **Coding Techniques for Implementing this, Policy.**

*[Add references to your site-specific guidelines for the different coding languages such as Perl, JAVA, C and/or Cpro.]*

1. **Policy Compliance**
   1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

* 1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

* 1. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Microsoft.

Any program code or application that is found to violate this policy must be remediated within a 90-day period.

1. **Related Standards, Policies and Processes**
   * Password Policy
2. **Definitions and Terms**

* Credentials
* Executing Body
* Hash Function
* LDAP
* Module

# Server Malware Protection Policy

**Overview**

Microsoft is entrusted with the responsibility to provide professional management of client’s servers as outlined in each of the contracts with its customers. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

**Purpose**

The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

**Scope**

This policy applies to all servers that Microsoft is responsible for managing. This explicitly includes any system for which Microsoft has a contractual obligation to administer. This also includes all server systems set up for internal use by Microsoft, regardless of whether Microsoft retains administrative obligation or not.

**Policy**

Microsoft operations staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

4.1 ANTI-VIRUS

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

Non-administrative users have remote access capability.

The system is a file server.

NBT/Microsoft Share access is open to this server from systems used by non-administrative users.

HTTP/FTP access is open from the Internet.

Other “risky” protocols/applications are available to this system from the Internet at the discretion of the Microsoft Security Administrator

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

Outbound web access is available from the system.

4.2 MAIL SERVER ANTI-VIRUS

If the target system is a mail server, it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

4.3 ANTI-SPYWARE

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet.

Any system where non-technical or non-administrative users can install software on their own.

4.4 NOTABLE EXCEPTIONS

An exception to the above standards will be granted with minimal resistance and documentation if one of the following notable conditions apply to this system:

The system is an SQL server.

The system is used as a dedicated mail server.

The system is not a Windows based platform.

**Policy Compliance**

Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

**Exceptions**

Any exception to the policy must be approved by the Infosec team in advance.

**Non-Compliance**

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None.

Definitions and Terms

The following definition and terms can be found on the Definitions and Terms page:

* **Malware**
* **Spyware**

# Server Audit Policy

Overview

See Purpose.

Purpose

The purpose of this policy is to ensure all servers deployed at Microsoft are configured according to the Microsoft security policies. Servers deployed at Microsoft shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

Ensure integrity, confidentiality and availability of information and resources.

Ensure conformance to Microsoft security policies.

Scope

This policy covers all servers owned or operated by Microsoft. This policy also covers any server present on Microsoft premises, but which may not be owned or operated by Microsoft.

Policy

Microsoft hereby provides its consent to allow Microsoft Auditing to access its servers to the extent necessary to allow Microsoft to perform scheduled and ad hoc audits of all servers at Microsoft.

Specific Concerns

Servers in use for Microsoft support critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability, or integrity of these systems.

Guidelines

Approved and standard configuration templates shall be used when deploying server systems to include:

All system logs shall be sent to a central log review system.

All Sudo / Administrator actions must be logged.

Use a central patch deployment system.

Host security agents such as antivirus shall be installed and updated.

Network scan to verify only required network ports and network shares are in use.

Verify administrative group membership.

Conduct baselines when systems are deployed and upon significant system changes.

Changes to the configuration template shall be coordinated with approval of the change control board.

Responsibility

Microsoft Auditing shall conduct audits of all servers owned or operated by Microsoft. Server and application owners are encouraged to also perform this work as needed.

Relevant Findings

All relevant findings discovered because of the audit shall be listed in the Microsoft tracking system to ensure prompt resolution or appropriate mitigating controls.

Ownership of Audit Report.

All results and findings generated by the Microsoft Auditing Team must be provided to appropriate Microsoft management within one week of project completion. This report will become the property of Microsoft and be considered company confidential.

Policy Compliance

Compliance Measurement

Microsoft Auditing shall never use the access required to perform server audits for any other purpose.

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

# Server Security Policy

1. **Overview**

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

1. **Purpose**

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Microsoft. Effective implementation of this policy will minimize unauthorized access to Microsoft proprietary information and technology.

1. **Scope**

All employees, contractors, consultants, temporary and other workers at Microsoft and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Microsoft or registered under a Microsoft-owned internal network domain.

This policy specifies requirements for equipment on the internal Microsoft network. For secure configuration of equipment external to Microsoft on the DMZ, see the Internet DMZ Equipment Policy.

1. **Policy**
   1. **General Requirements**
      1. All internal servers deployed at Microsoft must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs, and approved by the InfoSec team. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

* Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  + Server contact(s) and location, and a backup contact
  + Hardware and Operating System/Version
  + Main functions and applications, if applicable
* Information in the corporate enterprise management system must be kept up to date.
* Configuration changes for production servers must follow the appropriate change management procedures.
  + 1. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.
  1. **Configuration Requirements**
     1. Operating System configuration should be in accordance with approved InfoSec team guidelines.
     2. Services and applications that will not be used must be disabled where practical.
     3. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
     4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
     5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
     6. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
     7. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
     8. Servers should be physically located in an access-controlled, secure environment.
     9. Servers are specifically prohibited from operating from uncontrolled or unsecured cubicle areas.
  2. **Monitoring**
     1. All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
* All security related logs will be kept online for a minimum of 1 week.
* Daily incremental tape backups will be retained for at least 1 month.
* Weekly full tape backups of logs will be retained for at least 1 month.
* Monthly full backups will be retained for a minimum of 2 years.
  + 1. Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
* Port-scan attacks
* Evidence of unauthorized access to privileged accounts
* Anomalous occurrences that are not related to specific applications on the host.

1. **Policy Compliance**
   1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

* 1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

* 1. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1. **Related Standards, Policies and Processes**

* Audit Policy

1. **Definitions and Terms**

The following definition and terms can be found on the Definitions and Terms page:

* De-militarized zone (DMZ)

# Application Security Policies

# Software Installation Policy

1. **Overview**

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization’s network are examples of the problems that can be introduced when employees install software on company equipment.

1. **Purpose**

The purpose of this policy is to outline the requirements around installation software on Microsoft computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Microsoft computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

1. **Scope**

This policy applies to all Microsoft employees, contractors, vendors, and agents with Microsoft-owned mobile devices. This policy covers all computers, servers, smartphones, tablets, and other computing devices operating within Microsoft.

1. **Policy**
   1. Employees may not install software on Microsoft computing devices operated within the Microsoft network.
   2. Software requests must first be approved by the requester’s manager and then be made to the Information Technology department or Help Desk in writing or via email.
   3. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester’s need.
   4. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.
2. **Policy Compliance**
   1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

* 1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

* 1. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1. **Related Standards, Policies and Processes**

None.

# Web Application Security Application

1. **Overview**

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

1. **Purpose**

The purpose of this policy is to define web application security assessments within Microsoft. Web application assessments are performed to identify potential or realized weaknesses because of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of Microsoft services available both internally and externally as well as satisfy compliance with any relevant policies in place.

1. **Scope**

This policy covers all web application security assessments requested by any individual, group, or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at Microsoft.

All web application security assessments will be performed by delegated security personnel either employed or contracted by Microsoft. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of Microsoft is prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

1. **Policy**

4.1 Web applications are subject to security assessments based on the following criteria:

4.1.1 New or Major Application Release– will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

4.1.2 Third Party or Acquired Web Application– will be subject to full assessment after which it will be bound to policy requirements.

4.1.3 Point Releases– will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

4.1.4 Patch Releases– will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

4.1.5 Emergency Releases– An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be conducted. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.1.6 Annual Review – all applications will be subject to a full annual review in its entirety to review potential risks of functionality and/or architecture.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of medium risk level or greater.

4.2.1 High– Any high-risk issue must be fixed immediately, or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high-risk issues are subject to being taken off-line or denied release into the live environment.

4.2.2 Medium– Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies limit exposure.

4.2.3 Low– Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

4.3.1 Full– A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of all discovered.

4.3.2 Quick– A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.

4.3.3 Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

* + - MSAT
    - Windows Defender
    - Other In-house Microsoft Tools

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

1. **Policy Compliance**
   1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

* 1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

* 1. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

1. **Related Standards, Policies and Processes**

[OWASP Top Ten Project](http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

[OWASP Testing Guide](http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf)

[OWASP Risk Rating Methodology](http://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)

# Definitions and Terms Page

* Application layer proxy - receives requests intended for another server and acts as the proxy of the client to obtain the requested service.

• Blogging - writing, photography, and other media that is self-published online.

• Credentials - information that identifies an account and keeps it secure, as username and password

• De-militarized zone (DMZ) - n computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy.

• Executing Body - the physical apprehension and detention of a person by law enforcement officials to conduct a court order

• Hacking - the gaining of unauthorized access to data in a system or computer.

• Hash Function - An algorithm that computes a value based on a data object thereby mapping the data object to a smaller data object.

• Honeynet - a decoy network that contains one or more honeypots

• Honeypot - Programs that simulate one or more network services that you designate on your computer's ports. An attacker assumes you are running vulnerable services that can be used to break into the machine. A honey pot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

• LDAP - A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.

• Module – in computer hardware it is a component that is designed for easy replacement and in software an extension to a main program dedicated to a specific function.

• Peer to Peer File Sharing - the distribution and sharing of digital media using peer-to-peer (P2P) networking technology.

• Phishing - The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website.

• Proprietary Information - information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.

• Ransomware - A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

• Social Networking Services - a type of online social media platform which people use to build social networks or social relationships with other people

• Spam - Electronic junk mail

# References

Used to find the correct teams/ verified apps for web security policies and teams to enact the ethics policy.

Microsoft. (n.d.). *Microsoft Careers*. Home | Microsoft Careers. https://careers.microsoft.com/v2/global/en/home.html

Microsoft. (n.d.). *Microsoft 365 products, Apps, and services: Microsoft 365*. Microsoft 365 Products, Apps, and Services | Microsoft 365. https://www.microsoft.com/en-us/microsoft-365/products-apps-services

Microsoft. (n.d.). *Legal compliance and ethics*. Microsoft Legal. https://www.microsoft.com/en-us/legal/compliance?SilentAuth=1&wa=wsignin1.0

# Definition References

Oxford. (n.d.). *Oxford languages and google - English*. Oxford Languages. https://languages.oup.com/google-dictionary-en/

SANS. (n.d.). *Glossary of cyber security terms*. Glossary of Security Terms | SANS Institute. https://www.sans.org/security-resources/glossary-of-terms/

# Picture References

Wikimedia Foundation. (n.d.). *File: Microsoft Logo (2012).SVG*. Wikipedia. https://en.m.wikipedia.org/wiki/File:Microsoft\_logo\_%282012%29.svg