Innominds

Innominds IT Policies – Handbook

This handbook contains a collection of IT Policies of Innominds. All employees are expected to review these policies, understand these policies, and practice them. Failure to practice these policies will have severe consequences including termination of employment.

June 25, 2021

TABLE OF CONTENTS

Internet Acceptable User Policy

Effective - July 1, 2021

Overview

This policy applies to every individual who uses Organizational information assets, and it sets out what the Organization considers to be the acceptable use of those assets.

Introduction

The Internet is an unregulated environment. The Organization will not be liable for any material viewed or downloaded. Use of the Internet must be consistent with the Organization's standards of business conduct and must occur as part of the normal execution of the employee's job responsibilities. Any breach of the IAUP may lead to disciplinary action and possibly termination of employment. Illegal activities may also be reported to the appropriate authorities. Employees may also be held personally liable for damages caused by any violations of this policy.

An internet usage policy provides employees with rules and guidelines about the appropriate use of company equipment, network, and Internet access. Having such a policy in place helps to protect both the business and the employee; the employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to or there could be serious repercussions, thus leading to fewer security risks for the business as a result of employee negligence. The Internet Usage Policy is an important document that must be signed by all employees upon starting work. Below is an Internet Usage Policy that covers the main points of contention dealing with Internet and computer usage.

This Internet Usage Policy applies to all employees of Innominds who have access to computers and the Internet to be used in the performance of their work. The use of the Internet by employees of Innominds is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through Innominds is a privilege and all employees must adhere to the policies concerning computers, Email, and Internet usage.

"Employee" includes all employees of the Organization as well as contractors, temporary staff and third parties that are granted access to Organizational information assets

Computer, Email and Internet usage

- Organizational User IDs, websites and e-mail accounts may only be used for Organizationally sanctioned communications.
- Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted
- Use of Internet/intranet/e-mail/instant messaging may be subject to monitoring for reasons of security and/or network management and users may have their usage of these resources subjected to limitations by the Organization.
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role
- All Internet data that is composed, transmitted and/or received by Innominds computer systems is considered to belong to Innominds and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties
- The equipment, services, and technology used to access the Internet are the property of Innominds and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections
- Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images

- All sites and downloads may be monitored and/or blocked by Innominds if they are deemed to be harmful and/or not productive to business
- The installation of software such as instant messaging technology is strictly prohibited

Unacceptable use of the internet by employees includes, but is not limited to

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via Innominds email service
- Using computers to perpetrate any form of fraud, and/or software, film or music piracy
- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask IT team for further guidance and clarification. All terms and conditions as stated in this document apply to all users of Innominds network and Internet connection. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted by the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by Innominds.

User compliance

The regulations mentioned in this internet usage policy are covered by Innominds and any breaches of the policy can be addressed by the IT administrator, who is given control to oversee what downloads and site browsing is occurring on the network and the Internet within the workplace, through a user-friendly interface.

The regulations mentioned in this internet usage policy are covered by Innominds and any breaches of the policy can be addressed by the IT administrator, who is given control to oversee what downloads and site browsing is occurring on the network and the Internet within the workplace, through a user-friendly interface.

Moreover, administrators can block sites and control downloads in real-time with Innominds categorization and filtering ability that covers over million websites, making it the ideal companion to an effective Internet Usage Policy.

Violations

Any violations of this security policy should be brought to the attention of the IT Infrastructure Manager, who will work with the appropriate individuals to rectify the problem.

Ownership / Responsibilities

IT Infrastructure Manager:

- Oversee the implications of above process
- Ensure this document remains current and is updated whenever changes to the process occur
- Review and approve change to this document

Director Technology Services:

- Review and approve changes to this document.

VERSION HISTORY

**List the latest changes at the top of the below table*

Version	Date	Author	Reason for change
v1.0	1/July/2021	2552(vgole)	New policy

Vulnerability Management Policy

Effective - July 1, 2021

Overview

IT resources can be exploited in order to steal sensitive data, damage systems, or deny access to those resources. Vendors, recognizing vulnerabilities in their products, create software patches and other strategies which are distributed to their customers. Diligent customers implement those patches and strategies to prevent successful attacks from hackers. Unfortunately, as technologies evolve, new vulnerabilities are discovered, which must in turn be mitigated. Some vulnerability can be managed only with add-on security software and other specialized tools.

Non-technical vulnerabilities may also exist in the way employees control access to sensitive data and computer systems.

Risks to the IT infrastructure must be actively managed. The tasks involved, which can be time-consuming and mundane, are never-the-less essential to the overall health of the IT enterprise and the safety of its data. All employees must take responsibility for reducing technical and non-technical risks.

Purpose

This Information Technology Policy directs the establishment of vulnerability management practices in order to proactively prevent the exploitation of vulnerabilities and potential loss of Innominds sensitive data. The Innominds System will create and document systematic and accountable practices to maintain control programs and applications, to evaluate installed and new devices and systems for vulnerabilities, and to mitigate other technical and non-technical vulnerabilities. The goals of this effort are to implement stronger protection for Innominds IT resources, ensure compliance with best practices, and reduce the impact of threats to the Innominds and its constituents.

Scope

This policy applies to all Innominds employees, administrators, contractors, systems, applications, networks and affiliates.

Policy

Roles and Responsibilities

All Innominds employees will control access to sensitive information in both electronic system and hardcopy format.

IT Team at Innominds and Security administrators will oversee, support, and assist with the maintenance and security of server and workstation operating systems, network device control programs, applications, and data within their assigned areas.

The IT team will track, acquire, vet and distribute software patches and updates for all approved operating systems, for network devices, and for those applications, which are system-wide implementations across Innominds. In addition, Innominds will provide guidance and support for reducing risk and mitigating vulnerabilities.
Responsible IT team will patch and update servers, end-user devices and network devices under Innominds management, using tools and code provided by Innominds or local tools for non-system-wide implementations. IT team will track, acquire, vet and install patches and updates in a timely manner. IT team will implement risk reduction strategies and will mitigate detected vulnerabilities.

Specific Provisions

Patch and Update Management

IT team will install only approved software. All installed software will be maintained in a timely manner at supported levels, with appropriate patches and updates, in order to address vulnerabilities and to reduce or prevent any negative impact on Innominds operations.

Email Threat Management
Innominds e-mail system will be actively managed for spam, malware and inappropriate content. Suspicious email will be quarantined to prevent disruption to the email system or network.

Internet Browser Threat Management
Internet access will have controls implemented to inform users about potentially malicious sites and actively stop access to known malicious sites.

Vulnerability Awareness Training
Vulnerability awareness training is required for all employees, contractors, consultants as part of a comprehensive education and awareness program.

Asset Classification and Inventory
IT team will maintain a master inventory of software and IT equipment, along with an asset classification system. Vulnerability management strategies appropriate to each asset class will be used.

End-user Device and Server Intrusion Detection and Prevention
All end-user devices and servers that access or store sensitive data will have technology deployed to prevent, detect, repair, and manage malicious software and unauthorized intrusions.

Sensitive Data Loss Prevention
IT resources that are used to access and store sensitive data will have technology deployed to verify the data is accessed, stored, copied, printed, transmitted, discarded and otherwise handled in a secure and authorized manner.

End-user Device and Server Vulnerability Scanning and Threat Mitigation
IT Resources used to access, transmit and store sensitive data will be periodically scanned to verify they are free of vulnerabilities and up to date with all software versions and patches.

Network Intrusion Detection and Prevention
INNOMINDS network is actively managed, and technology is deployed to detect and prevent unauthorized intrusion or access to sensitive data, and the transmission of malicious software or inappropriate content.

Log Management
Logs created by servers, firewalls, network devices, control programs and applications will be analyzed, secured and maintained for a period to assist with troubleshooting and forensic assessments.

File Integrity Management
Files containing sensitive data will be managed to ensure only appropriate access and authorized changes are allowed. When necessary, all access to files containing sensitive data will be logged and reviewed.

Network Vulnerability Scanning and Threat Mitigation

All changes to the network will be approved, recorded, monitored, and verified. The network will be actively managed to detect network vulnerabilities and unauthorized changes or extensions to the network.

Employee–related Vulnerabilities

Employees will adhere to approved standards and procedures for accessing, using and managing sensitive data and other IT resources.

Ownership / Responsibilities

IT Infrastructure Manager:

- Oversee the implications of above process
- Ensure this document remains current and is updated whenever changes to the process occur
- Review and approve change to this document

Director Technology Services:

- Review and approve changes to this document.

VERSION HISTORY

**List the latest changes at the top of the below table*

Version	Date	Author (ID/Name)	Reason for change
v1.0	01/July/2021	2552(vgole)	New policy

Application Security Policy

Effective - July 1, 2021

Overview

This document forms part of the suite of Security Policy documents for Innominds and IT services to all locations of Innominds.

The Authority will take appropriate steps to protect the IT environment from threats, including but not limited to unauthorized access, computer viruses, violation of privacy and interruption to service.

Purpose

This document lays down the minimum-security standard applicable to applications used in Innominds. All such application software is at high-risk, but some particularly high-risk systems will need to take additional security steps beyond those prescribed in this document.

This Application Security Policy applies to all information systems and information system components of the IT environment. Specifically, it includes:

- Servers and other devices that provide centralized computing capabilities
- SAN, NAS and other devices that provide centralized storage capabilities
- Desktops, laptops and other devices that provide distributed computing capabilities
- Routers, switches and other devices that provide network capabilities
- Firewalls, IDP sensors and other devices that provide dedicated security capabilities.

Scope

This policy applies to all Innominds employees, administrators, contractors, systems, applications, networks and affiliates.

Policy

In order to accurately create a security standard to control applications, it is necessary to first define the types of application software that will exist in Innominds. These may be categorized as follows:

Standard Applications

A standard application is one that is included on the list of permitted applications, contractually agreed by the Authority and its supplier(s). Specifically, applications of this nature will fall into one of three categories: Innominds Applications, Office Productivity Applications and Administration Applications.

New applications may be added to the list of Standard Applications on the request of the Authority and agreed with their supplier(s).

Control Statement: Standard documentation shall be produced describing the standard configuration of applications within the IT environment.

Control Statement: Deviations from the standard builds shall be documented.

Non-standard Applications

A non-standard application is a manually installed package that is not part of the contractually agreed application list. For example, this would include applications manually installed by a supplier on an ad-hoc basis at the specific request of a Innominds or the Authority. Applications of this type should follow the principles of the standard applications and may be reviewed by the Authority to see if they should become part of the standard applications list.

Non-standard Applications

Unauthorized software incorporates any piece of software that is installed on any workstation or server in a Innominds without the prior knowledge of the Authority or their supplier(s). This includes, but is not limited to, rogue software, Trojans, viruses, games, protocol analyzers, freeware, shareware, communication software, and any other software that permits or promotes hacking, system intrusion or system performance degradation.

The Information Security Manager reserves the right to remove software of this nature if it poses an issue on any system in a Innominds site.

Control of Applications

Due to the nature and variety of applications that will be used in the IT environment a measure of control over applications will be required to ensure continuity of service. Security, performance and availability may become compromised due to the introduction of non-standard or unauthorized software. In order to prevent disruption to service from such software, the following steps are required:

Control Statement: The IT Infrastructure Manager shall evaluate all new applications to determine their suitability for installation in the IT environment. Any application that is deemed unsuitable shall be rejected by the IT Infrastructure Manager and therefore not installed in any Innominds site.

Control Statement: Group policies shall be set such that ordinary users cannot normally install or remove applications from machines in the IT environment.

Control Statement: The IT Infrastructure Manager shall retain the right to remove any piece of software that is deemed unsuitable or unacceptable to the environment in any Innominds site. This includes any software on IT equipment that may impact availability or key performance indicators.

Control Statement: The installation of unauthorized software is not permitted on any server or workstation.

Control Statement: The IT Infrastructure Manager shall keep a list of software that is not permitted and may amend this list at any time.

Control Statement: The A list of all authorized software licenses will be maintained.

In order to comply with legal requirements, only licensed software will be installed on machines.

Application-level Authentication

Some applications require their own authentication within the application. Where possible, they should not use an embedded authentication database in order to limit the number of places authentication information is stored, however it is accepted that most of the chosen database applications behave in this way.

Control Statement: Where possible, applications that require authentication should be configured to use Windows Active Directory authentication or equivalent directory service.

Control Statement: The Authority must ensure that default passwords on databases with embedded authentication are changed after installation.

Control Statement: Default passwords on applications are to be changed on first login.

Control Statement: Passwords within Applications must have the appropriate complexity as defined in the password policy.

Control Statement: Where possible, establish a unique identifier and secret information for each application - but as a minimum establish a unique identifier for each application.

Control Statement: The application should be identified to the system.

Control Statement: Access to application system files should be controlled.

Changes to Application Software

From time to time, software patches and upgrades are issued to application software, to fix performance and security issues, and to enhance functionality. Critical updates shall be applied to all applicable machines in a timely manner.

Control Statement: All changes to the existing standard software builds and application software shall be made in compliance with applicable Change Control Procedures.

Control Statement: All patches and upgrades to the existing standard software builds and application software will be tested before they are applied to production environment and machines.

Control Statement: The IT Infrastructure Manager will ensure that all critical patches are applied in a timely, managed and controlled manner.

Critical Application Parameters and Resource Configuration

Application Service Accounts

Some applications will require a Microsoft Windows service account, application logon account or Windows logon account. These accounts must be subject to the same security rules as the operating system accounts.

Control Statement: Accounts used by applications shall have passwords of at least 10 characters in length and require a combination of alpha numeric text.

Control Statement: The Authority shall ensure that accounts used by applications must not use the default password provided for that application after the installation process.

Control Statement: Accounts used by applications should not use the default username provided for that application.

Control Statement: Critical applications using Windows Account passwords shall be configured with the 'Password Never Expires' flag set.

Control Statement: Accounts used by applications shall be given the least possible privileges and rights necessary to allow the required functionality of the applications.

Control Statement: Where privileges and rights are granted to accounts used by applications, these privileges and rights are to be reviewed on regular basis to ensure that privileges and rights that are no longer required are removed.

Application Service Accounts

Security must be included in the design, development or deployment of an application. Development processes should follow generally accepted standards of good practice. Risk assessment should be conducted to ensure that the proposed application will not introduce risk to the IT environment and Information assets.

Control Statement: Secure coding practices shall be followed for all application development.

Control Statement: When developing applications, input, output and processing validation assessment must be undertaken to ensure information is not corrupted during processing.

Control Statement: Applications will be subject to testing prior to being introduced to live environment, to ensure that data is being processed correctly, ensuring the integrity of the data being input, processed and output.

Control Statement: During development and testing, applications shall not have access to live production data.

Control Statement: Change control procedures are to be followed when implementing the application into Live environment.

Software Maintenance

Only authorized software maintenance personnel will be permitted to carry out maintenance tasks. This will be ensured by controls including:

Control Statement: The identity of software maintenance personnel must be checked immediately on arrival and before any physical access is permitted.

Control Statement: A contract must exist with the software maintenance company prior to any work being carried out; and

Control Statement: Normal operating controls such as supervision, restriction of access to operational data, and controls over the ability to take soft or hard copies of the data, will apply

Waiver from Policy

Request for a waiver from this Information Policy must be address to the IT Infrastructure Manager. The request for a waiver must describe why a waiver is required, justification why the policy cannot be adhered to, and a plan to bring the application or system into compliance in the future. The IT Infrastructure Manager will discuss waiver requests with senior management, as appropriate. Waivers can be granted by the IT Infrastructure Manager for a period not exceeding one year, but may be extended annually if the justification still applies.

Monitoring and Review

The IT Infrastructure Manager is responsible for monitoring and reviewing this policy and will conduct a formal review of the efficiency and effectiveness of its application on an annual basis.

Violations

Any violations of this security policy should be brought to the attention of the IT Infrastructure Manager, who will work with the appropriate individuals to rectify the problem.

Ownership / Responsibilities

IT Infrastructure Manager:

- Oversee the implications of above process
- Ensure this document remains current and is updated whenever changes to the process occur
- Review and approve change to this document

Director Technology Services:

- Review and approve changes to this document.

VERSION HISTORY

**List the latest changes at the top of the below table*

Version	Date	Author (ID/Name)	Reason for change
v1.0	01/July/2021	2552(vgole)	New policy

Firewall Policies

Effective - Jun 1, 2021

Overview

Network Security Services (NSS), a department of IT Technology, operates a firewall to enhance security between the Internet and the Innominds network to establish a reliable network for the Innominds computer and network resources. The Firewall is a key component of the Innominds network security architecture.

This Firewall Policy governs how the firewall will filter Internet traffic to mitigate the risks and losses associated with security threats to the Innominds network and information systems. This policy will attempt to balance risks incurred against the need for access.

Purpose

A firewall is one element of security for Innominds network. It reduces the threat of outsiders either damaging Innominds systems or using the systems as a jumping off point for illegal entry into other systems. A firewall does not prevent malicious or illegal activities from inside the firewall.
This policy is designed to protect Innominds computers (Owned/Client) from hacking and virus attacks by restricting access to computers on Innominds from users who are off location.

Scope

This policy applies to all Innominds employees, administrators, contractors, systems, applications, networks and affiliates.

Definitions

Firewall

A Firewall is a hardware and software device that controls access between two networks. There are several different mechanisms for performing this access control, but the essential point is that a firewall implements a network security policy.

Firewall System

A firewall system includes both the Firewall Product and additional controls, that may or may not be available as part of the base firewall product. Typically, these can comprise solutions to block or filter content, e.g., anti-virus email gateways, intrusion detection systems, audit and logging tools, mobile code (ActiveX, Java) monitors, integrity checkers, email content scanners and URL blockers.

Responsibilities

Network Security Services is responsible for implementing and maintaining Innominds network perimeter firewall. Therefore, NSS is also responsible for activities relating to this policy. Responsibility for information systems security on a day-to-day basis is every employee's responsibility. Specific guidance and direction for information systems security is the responsibility of NSS.

Policy

The Firewall permits the following for outbound and inbound Internet traffic:

- Outbound- Allow ALL Internet traffic to hosts and services outside of Innominds with the exception of known security vulnerabilities (see below). This allows anyone connected to Innominds Network to utilize all services on the Internet with the exception of known vulnerabilities.

- Inbound- Only specific services which support Innominds organization will be allowed to be accessed from the Internet. The chart below identifies the most common services used for Internet communications within Innominds environment.

The following is a limited explanation for each column:

- **Server Functions and Services** - This a listing of the most common Internet services used on the Innominds servers to support the mission and business of the Innominds.
- **Innominds Network to Internet** - All traffic originating from a Innominds computer to an external host has no firewall policies applied except for known security vulnerabilities which are described in the chart below.
- **Internet to Innominds Network** - All traffic originating from a computer on the Internet (some where off-campus) to a computer on Innominds network is only allowed into the following systems.

Innominds Network to the Internet: Services which are NOT allowed	Internet to Innominds Network: Services which are NOT allowed
• Virus Related Protocols • Network Monitoring Protocols • Spyware Related Protocols (MarketScore Spyware)	• E-mail Server • Web Server • Blackboard • SSS (FTP Only) • Software (FTP Only) • Web Advisor • Library Catalog and Databases • Remote Desktop to Any OSX and Windows XP System • Other Departmental Servers • Web Helpdesk • Terminal Services • Library Catalog Search • Remote Desktop (as needed)

Operational Procedures

Only firewall system administrators are permitted to logon to the firewall.

- Access to firewall hosts must be tightly controlled. Only firewall system administrators are allowed to have user accounts on firewall hosts.
- Firewall system administrators must have personal accounts, i.e. no group logins are allowed.
- Direct remote root access is not allowed. All root access must be via a personalized logon.
- Only personnel with the appropriate authorization can make changes to the firewall access rules, software, hardware or configuration.
- All changes should be as a result of a request recorded using the Firewall Change
- Request Form although emergency modifications can be requested by phone, with a follow up email and change request.
- Only authorized personnel must be able to implement the changes and an audit log must be retained.

ONLY AUTHORISED departmental technical contacts may request any changes to Innominds firewall. These requests must be submitted in writing or electronic including a rationale for the request by submitting the Firewall Change Request Form.

The Security Coordinator of IT Security will evaluate the risk of opening the firewall to accommodate requests. Where the risk is acceptable, granting of requests will be dependent on network infrastructure limitations and the availability of required resources to implement the request. If the risk associated with a given request is deemed objectionable, then an explanation of the associated risks will be provided to the original requestor and alternative solutions will be explored.

If during the implementation it is determined that the original request does not provide the functionality to meet the unit's business need, then the Security Manager of NSS has the authority to deny the request.

NSS will, on a short-term basis; provide open access through the firewall. Subsequently, long-term, the NSS will work with the requestor to determine exactly what ports are needed to meet the unit's business needs. Certain mission-critical functions require outside vendors and other entities to have secured and limited access to departmental network resources from the Internet to Innominds. This access needs to be approved by the department technical contact and then coordinated through NSS by submission of the Firewall Change Request Form.

If the original requestor considers the solution to be unsatisfactory, the request may be appealed to IT Infrastructure Manager.

Turnaround time for a request for a normal change request will be handled in approximately 5 business days from the receipt of the Firewall Change Request Form. Common Services include:

- FTP
- Telnet/SSH
- Mail
- Remote Access
- SMTP
- HTTP/HTTPS

Turnaround time of a request for any emergency request will be handled as quickly as possible. To be an emergency the change must correct a major security risk. This additional time is needed to investigate that risk associated to Innominds Network.

Operational Procedures

The firewall will be configured to deny any service unless it is expressly permitted.

- If there are no rules defined for Innominds network address, then traffic to or from that address must be denied.
- Access to the Innominds network must be blocked during the start-up procedure of the firewall.
- The firewall Operating System will be configured for maximum security.
- The underlying operating systems of firewall hosts must be configured for maximum security, including the disabling of any unused services.
- The firewall product suite must reside on dedicated hardware.
- Applications that could interfere with, and thus compromise, the security and effectiveness of the firewall products, must not be allowed to run on the host machine.
- The initial build and configuration of the firewall must be fully documented.
- This provides a baseline description of the firewall system to which all subsequent changes can be applied. This permits tracking of all changes to ensure a consistent and known state is maintained.
- Security must not be compromised by the failure of any firewall component.
- If any component of the firewall fails, the default response will be to immediately prevent any further access, both "outbound" as well as "inbound".
- A firewall component is any piece of hardware or software that is an integral part of the firewall system. A hardware failure occurs when equipment malfunctions or is switched off. A software failure can occur for many reasons e.g., bad maintenance of the rules database on the firewall or software which is incorrectly installed or upgraded.
- IP forwarding at the operating system level must be disabled until the firewall software is operational and IP filtering policies active.

Audit and Compliance

Regular testing of the firewall shall be carried out.
The firewall must be regularly tested for:

- configuration errors that may represent a weakness that can be exploited by those with hostile intent.
- consistency of the firewall rule set, i.e. to confirm the current status matches that expected (and documented).

- secure base system implementation: i.e. the integrity of the firewall hosts and applications must be verified using an integrity-checking tool

The firewall system must have an alarm capability and supporting procedures

- When an agreed specified event occurs, an alarm must be sent to the security personnel. Documented procedures must exist to permit an efficient response to such firewall security alarms and incidents.
- There may be specific circumstances when it would be advantageous for the firewall system to react in an automated manner to defined security events.
- If the firewall itself is the subject of malicious attempts to penetrate it, and the firewall has the capability, delivery of services should be terminated rather than permit uncontrolled access to the Innominds network.

There must be an active auditing/logging regime to permit analysis of firewall activity either during or after a security event

- An audit trail is vital in determining if there are attempts to circumvent the firewall security.
- Audit trails must be protected against loss or unauthorized modification.
- The firewall system must be able to provide logging of specific (or all) traffic when suspicious activity is detected.

Compliance Requirements

These guidelines are intended to supplement, not replacing all existing policies, regulations, agreements and contracts that currently apply to Innominds computing and networking services.
Persons given access to the department's technology and information assets must sign a statement that they have read and agree to abide by this policy.

Periodic Review of Firewall Security Policies

Firewall security policies will be reviewed at least yearly. When there are major changes to the network requirements this may warrant changes to the firewall security policy.

OWNERSHIP / RESPONSIBILITIES

IT Infrastructure Manager:

- Oversee the implications of above process
- Ensure this document remains current and is updated whenever changes to the process occur
- Review and approve change to this document

Director Technology Services:

- Review and approve changes to this document.

VERSION HISTORY

**List the latest changes at the top of the below table*

Version	Date	Author (ID/Name)	Reason for change
v1.0	01/Jun/2021	2552(vgole)	New policy

Instructions for Innominds Firewall Change Request Form

Only authorized contacts can request firewall changes.

Innominds Firewall Change Request Form should be completed by authorized firewall change request authority. Sections 1-10 at the top of the page should be completed by the department requesting modifications to Innominds firewall.

1. Requester's Name (Printed): Enter the name of the person making the firewall change request.
2. Requester's Phone #: Enter the phone number of the contact person for the request.
3. Requester's Email: Enter the email address of the contact person for the request. (Must be a Innominds email address)
4. Department: Enter the department name of the person making the request.
5. Project: Enter the project name of the person making the request.
6. Change Category: Mark the change category.
7. A normal change request will be handled within five (5) working days.
8. An emergency change request will be handled as quickly as possible. To be an emergency the change must correct a major security risk.
9. Proposed Change Date: Enter the date changes to the firewall should be applied. If changes do not need to be applied on a specific day leave this field blank.
10. Description of what you are trying to accomplish: Enter a brief description of what is to be accomplished with the firewall rule change. If necessary, attach additional pages.
11. Authorized Requester's Signature, Title: Enter the signature and job title of the authorized department contact. If the form is submitted by email a signature is not required, but the email must originate from an authorized contact's email address.
12. Date: Enter the date of signature.

The bottom portion of the form will be completed by the Network Security staff. The form should be submitted or **emailed to ticket@innominds.com** Conformation of the completion of the requested change will be made to the requester by phone or email.

Laptop Care Guide

Version 1.0

Effective - June 1, 2021

1.0 Overview

Laptop computers provide important functionality, allowing employees to have their computing resource at hand in meetings/workplace or even at home in certain time pressing situations so as to enable employees to be maximally functional and productive while away from office premises.

2.0 Scope

This Policy and the procedures herein affect all employees who use laptops for official purposes. Employees are also advised that in addition to the terms and conditions of laptop care as reflected in this Policy, employees shall also have to adhere to any terms of their respective employment agreement which mandate or restrict any action in this regard.

An employee using company provided laptops is responsible for the care of that laptop, regardless of whether the laptop is used in the office, at one's place of residence, or in any other location such as a hotel, conference room or while travelling. This Policy contains certain guidelines and restrictions on the usage of the laptop that are required to be strictly adhered to by all employees while using these laptops.

3.0 Guidelines

You are responsible for protecting your laptop from loss or theft and for protecting the information it contains. These rules are provided to assist in assuring that your laptop is always secure. All conceivable situations cannot be covered in this document. Associates must realize that common sense should be your guide when faced with unusual or unforeseen situations.

- Operate your laptop on a safe and stable environment. Do not place on uneven or unstable work surfaces. Placing your laptop on the floor where it can be stepped on or kicked should also be avoided. Seek servicing if the casing has been damaged. Keep your computer centered on your desk. It should not hang off the edge.
- Keep liquids away from your laptop. As tempting as it might be to drink coffee, soda or any other liquid near your laptop, accidents can happen all too easily. Spilled liquids may damage the internal components or cause electrical injury to the laptop. Short circuits can corrupt data or even permanently destroy parts. The solution is very simple: Keep your drinks away from your computer. Even if you're careful, someone else might bump into your desk or you.
- Protect the screen (LCD) and body of your laptop. Do not place or drop objects on top and do not shove any foreign objects into the Notebook PC. When you shut your laptop, make sure there are no small items, such as a pencil or small earphones, on the keyboard. These can damage the display screen when shut; the screen will scratch if the item is rough. Close the lid gently and holding from the middle. Closing the lid using only one side causes pressure on that hinge, and over time can cause it to bend and snap.
- Keep food away from your laptop. Don't eat over your laptop. The crumbs can go down between the keys in the keyboard and provide an invitation to small bugs. The crumbs can also irritate the circuitry. Worse, it makes the laptop look dirty if there are crumbs and food stains on it. Always have clean hands when using your laptop. Clean hands make it easier to use your laptop touchpad and there will be less risk of leaving dirt and other stains on the computer. In addition, if you clean your hands before use, you will help reduce wear and tear on the coating of the laptop caused by contact with sweat and small particles that can act upon the laptop's exterior underneath your wrists and fingers.
- Protect the LCD display monitor. When you shut your laptop, make sure there are no small items, such as a pencil or small earphones, on the keyboard. These can damage the display screen when shut; the screen will scratch if the item is rough. Close the lid gently and holding from the middle.

Closing the lid using only one side causes pressure on that hinge and over time can cause it to bend and snap. Do not press or touch the display panel. Do not place together with small items that may scratch or enter the Notebook PC.

- Don't leave your laptop in a car. Not only do the insides of cars experience large temperature swings that could damage a laptop, but a laptop (or laptop bag) is an inviting target for a smash and grab thief.
- Don't expose your laptop to rapid temperature fluctuations. When bringing your laptop indoors from a cold environment, don't turn it on immediately. Instead, let it warm to room temperature first. This will avoid any potential for damage to the disk drive from condensation forming inside the machine.
- Don't pull on the power cord. Tugging your power cord out from the power socket rather than putting your hand directly on the plug in the socket and pulling can break off the plug or damage the power socket. Also, if you have the power point near your feet, avoid constantly bumping into the plug or you could loosen it and eventually break it. Do not expose to strong magnetic or electrical fields. Don't roll your chair over the computer cord. Stick the cord onto your desk with tape or a special computer cord tie which can be easily undone when you've finished using the laptop. Always try to keep most of the cord away from the floor or your legs; sometimes you can be so engrossed in what you're doing that you move your legs and forget the cord is there.
- Hold and lift the computer by its base, not by its LCD display (the screen). If you lift it by the screen part alone, you could damage the display or the hinges attaching it to the base. The display is also easily scratched or damaged by direct pressure – avoid placing pressure on it.
- Use a properly sized laptop case. Whatever you use to carry your laptop around in, be it a case, a bag or something you have made yourself, make sure that it is large enough to contain the laptop. This will avoid scratching, squeezing or even potentially dropping it. Use your TAS laptop bag when carrying your laptop. Many breaks happen because of laptops being dropped or bumped. A bag greatly reduces the risk of damage.
- Most laptop batteries will last at least two to three hours when fully charged. So, users don't need to have their laptops plugged in all the time. Therefore, users can unplug their adapter chargers every hour or so for about 15 minutes. That will give the adapter a 15-minute cool off period every hour. However, the adapter will still be plugged in most of the time to keep the battery charged for those periods when the laptop isn't plugged in.
- The most effective way to protect your computer from a power surge is to use a surge protector. Not to be confused with a power strip, a surge protector is a device with one or more outlets in which you plug electronic devices to protect them from power surges. Rather than plugging your computer directly into a wall outlet, for example, you can plug it into a surge protector. You can then plug the surge protector into the wall outlet to keep your computer safe from power surges.
- If a power surge occurs, the surge protector will do one of two things to protect your computer from potentially catastrophic damage:
    - Block the additional voltage
    - Short the additional voltage

4.0 Care tips

- Be sure to store the laptop in a safe place and be sure nothing is stacked or thrown on top of the laptop case.
- Power off your laptop whenever it is not in use. Do not carry the laptop in suspend or hibernation mode.
- Place your laptop on a sturdy work surface clear of all food, drink, and sharp obstacles.
- Don't place anything between the screen and keyboard when you close the computer.
- Be careful with your charger. Don't roll over, step on or "yank" the cord. Keep your charger in a separate area from your laptop. If you carry your charger in your laptop case, be careful when you lay your laptop case down. Be sure the charger is on the top to keep the screen from cracking.
- Do not pick at your laptop keys or remove them for any reason.
- Don't leave a pen or pencil on your laptop when you close it.

- Condition your laptop battery, meaning charge and drain your battery a few times when you first get it.
- Use a soft cotton cloth, such as a handkerchief, moistened with non-alkaline detergent to clean your computer.
- Do not place your laptop on a pillow or other soft material when it's on, because this may block the airflow vents on the bottom of the laptop and cause the computer to overheat.
- When using your laptop or charging the battery, it is normal for the bottom of the case to get warm. For extended use, place the computer on a hard flat surface. The bottom of the laptop case acts as a cooling surface that transfers heat.
- Be sure to unplug your laptop if there is an electrical storm.
- Keep the notebook free of dust and crumbs. Dust can cause a notebook to overheat. Use a can of compressed air to blow dust away from ports and the keyboard. Wash hands before touching the keyboard to avoid dirty or sticky keys. Invest in a microfiber cloth to clean the LCD screen.

VERSION HISTORY

**List the latest changes at the top of the below table*

Version	Date	Author	Reason for change
v1.0	01/June/2021	2552(vgole)	New policy

Innominds Password Policy

Version 2.0
Effective - Sept 25, 2017

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Innominds' entire network. As such, all Innominds employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 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 Innominds facility, has access to the Innominds network, or stores any non-public Innominds information.

4.0 Policy

4.1 General

- All system-level passwords must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every month
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords should not be sent a to group email ID or group of people in an email.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Innominds. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, device logins and IT access logins. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, date month year combinations, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "Innominds", "software", "Im" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9 ,!@#$%^&*()_+|-=\`{}[]:";'<>?,./)
- **Exceptions of usage of special characters are only limited to the applications**
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "One way I can remember my password" and the password could be: "Ow1crMp#" or "1Wic?mp/" or some other variation.

B. Password Protection Standards

Do not use the same password for Innominds accounts as for other non-Innominds access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Innominds access needs. Do not share Innominds passwords with anyone, including administrative assistants or secretaries.

All passwords are to be treated as sensitive, confidential Innominds information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in **an email message**
- Don't reveal a password to your supervisor
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Technology (IT).

Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, Instant Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once month (except system-level passwords which must be changed quarterly).

If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- should support authentication of individual users, not groups.
- should 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.

D. Remote Access

Access to the Innominds Networks via remote access is controlled using Virtual Private Networking (VPN). VPN client software is available from IT.

E. Passwords at Account Creation

When a request for a username is requested, IT staff will determine the type and privileges required. The password will be set to be pre-expired so the user will be required to change their password when they first successfully logon to the system. The lifetime of the password will be set according to the guidelines set in section 4.1 of this document.

F. Forgotten Passwords

Users will occasionally forget their password. A characteristic of password files is that passwords cannot be looked up. If a user forgets their password, the password can be changed by IT staff with the below guidelines.

- The user must present a photo id to the IT staff member before the password will be changed.
- Users who cannot contact IT in person should call IT mention and request a call back on the number.

- IT staff will call back again on the number specified and ask for the employee's manager domain ID and department name/ID.
- Once confirmed IT staff will generate a 10-digit random password with change over the first logon set and send out to the user via registered personal email.
- An email must be sent to the manager and the user again without the password notifying them to contact IT immediately if the password is not initiated by the user.

5.0 Enforcement

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

VERSION HISTORY

**List the latest changes at the top of the below table*

Version	Date	Author	Reason for change
v1.0	01/April/2016	1854(sbattar)	New policy
V2.0	25/Sept/2017	1854(sbattar)	Policy revision

Innominds Password Policy – Dos and Don'ts

Version 2.0
Effective - Sept 25, 2017

Dos and Don'ts - outlined as part of Innominds' IT Policies & Guidelines

Innominds IT team has shared the responsibility of every employee and business unit as a shared responsibility. YOU play a key role in properly safeguarding and using customer, private, sensitive information and company resources. The following **Dos and Don'ts** are to help remind us all of actions we must take to remain vigilant.

- DO use hard-to-guess passwords or passphrases. A password should have a minimum of 10 characters using uppercase letters, lowercase letters, numbers and special characters. To make it easy for you to remember but hard for an attacker to guess, create an acronym. For example, pick a phrase that is meaningful to you, such as "My son's birthday is 12 December, 2004." Using that phrase as your guide, you might use Msbi12/Dec,4 for your password.
- DO Reset default Wi-Fi router passwords while working from home since it is the door for hackers.
- DO keep your passwords or passphrases confidential. DON'T share them with others or write them down. You are responsible for all activities associated with your credentials.
- DON'T leave sensitive information lying around the work area/public place. DON'T leave printouts or portable media containing private information around the work area/public place. Lock them in a drawer to reduce the risk of unauthorized disclosure.
- DON'T post any private or sensitive information, such as passwords or other private information, on public sites, including social media sites, and DON'T send it through emails. DO use privacy settings on social media sites to restrict access to your personal information.
- DO pay attention to phishing traps in email and watch for telltale signs of a scam. DON'T open mail or attachments from an untrusted source. If you receive a suspicious email, the best thing to do is to delete the message, and report it to your manager and IT..
- DON'T click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks.
- Beware of phishing emails, to avoid use of public Wi-Fi, to ensure home Wi-Fi routers are sufficiently secured and to verify the security of the devices that they use to get work done

It is likely that attempts to subvert security using phishing attacks will increase at this time.

- DON'T be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner. DON'T respond to phone calls or emails requesting confidential data.
- DON'T install unauthorized programs on your work computer. Malicious applications often pose as legitimate software.
- DON'T plug in portable devices(USB sticks) at all without permission from your IT team. These devices may be compromised with code just waiting to launch as soon as you plug them into a computer. There have been too many examples of such devices being infested with malware.
- DO lock your computer when not in use. This protects data from unauthorized access and use.
- Installation of third-party apps should be confined to Bonafede app stores, even on personal devices.
- DON'T leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured. If a device is lost or stolen, report it immediately to your manager and IT team.
- DO remember that wireless is inherently insecure. Avoid using public Wi-Fi hotspots. When you must, use company provided virtual private network software to protect the data and the device.
- DON'T leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment.

- DO report all suspicious activity and cyber incidents to your manager and IT team. Part of your job is making sure client data/client code is properly safeguarded, and is not damaged, lost or stolen.
- DO ensure to take your laptop backed up to One drive.
- DO ensure to install the required VPN setup while in office itself before going on WFH.

VERSION HISTORY

**List the latest changes at the top of the below table*

Version	Date	Author	Reason for change
v1.0	01/April/2016	1854(sbattar)	New policy
V2.0	25/Sept/2017	1854(sbattar)	Policy revision

Confidentiality & Information Security Agreement

Version 1.0 Effective - Sept 1, 2018

I understand and acknowledge that failure to comply with this agreement may result in the termination of my employment or association with Innominds.

I agree to:

- Not disclose confidential or proprietary information to any individuals who are not authorized to receive the information or to those who do not have a legitimate need to know to carry out their duties at Innominds.
- Protect the privacy and confidentiality of the information and not disclose or share any confidential of our clients, employees, contractors associated with Innominds.
- Not access, change or destroy confidential or proprietary information except as required to perform the job assigned.
- Know that the user of Innominds Information Systems to access the confidential information may be audited and that Innominds may take away access at any time.
- Dispose of documents or other media when no longer needed, in an approved manner that protects confidentiality and follow the correct procedures where applicable.
- Access only levels or components of Information System as assigned to perform the job or service.
- Keep password(s) secret and not share with anyone. If I suspect that the password is known, immediately notify the IT department and change it so as not compromise computer security
- Not install, transmit or download from the Internet into any Information System of Innominds, any unauthorized or unlicensed software, or material protected by copyright.
- Not make unauthorized copy of Innominds Intellectual Property.
- Log-off or secure workstation, when unattended, according to the IT Policy.
- Adhere to warnings about the computer viruses and perform virus scan updates as directed.
- Not transmit or display abusive, discriminatory, harassing, inflammatory, profane, pornographic or offensive language or other such materials over or on any Innominds Information Systems.
- Report log-on or other systems problems to the Innominds IT team via ticket@innominds.com
- Use Innominds Information Systems wisely to conserve the costly space on the servers.
- Abide by the provisions of agreement if granted remote access to any Innominds Information System
- Use Innominds Information System equipment for the sole purpose of performing the assigned task or job.
- Immediately report any violations of these provisions to Innominds manager
- Participate in ongoing Information Security Training as directed

Employee Name:	Authorized By:
Signature:	Date:
Issued By:	Place: