Information Security Policies Handbook

Reference Guide

Russell Camilleri

19th September 2021

Contents

Information Security Policies Handbook

The policies within this handbook are based on the SANS institute which specializes on cyber security (SANS, 2021). Furthermore, an additional policy specifically intended for PCI compliance is included in the policy (Wilder, 2020).

Table 1 - Revised information security policies

Policy #	Policy name	Purpose
INFOSEC01	Acceptable encryption	Defining a standard for the use of acceptable encryption mechanism within the organization.
INFOSEC02	Acceptable use	Defining a standard for the use of IT related systems within the organization.
INFOSEC03	Bluetooth baseline requirements	Defining a standard for the use of Bluetooth enabled devices connected to company network and/or devices.
INFOSEC04	Clean desk	Defining a standard for the safekeeping of sensitive/critical information from an end user workspace.
INFOSEC05	Data breach response	Defining a standard process which needs to be followed in a data breach incident.
INFOSEC06	Database credentials coding	Defining the requirements to securely store database credentials.
INFOSEC07	Digital signature acceptance	Defining a standard for the acceptance digital signature as valid identification.
INFOSEC08	Disaster recovery plan	Defining a standard process which needs to be followed in a disaster recovery incident.
INFOSEC09	End user encryption key protection	Defining the requirements for safeguarding encryption keys managed by end users.
INFOSEC10	Ethics	Defining the company’s culture towards openness, trust and customer centricity through an ethical code of conduct.
INFOSEC11	Information logging standard	Defining the audit log requirements of systems within the organization.
INFOSEC12	Lab security	Defining the requirements to manage lab environments.
INFOSEC13	Minimum access	Defining a standard to provide minimal system access for users.
INFOSEC14	PCI compliancy	Defining a baseline configuration for systems regulated within PCI compliance.

Table 2 - Revised information security policies (continued)

Policy #	Policy name	Purpose
INFOSEC15	Pandemic response planning	Defining a response plan in case of a pandemic, affecting the majority of the workforce, thus ensuring business continuity.
INFOSEC16	Password construction	Defining a standard for the creation of strong password through best practices.
INFOSEC17	Password protection	Defining a standard for the protection of strong password.
INFOSEC18	Remote access	Defining a standard for remote access to the organization's network and systems.
INFOSEC19	Remote access tools	Defining the requirements to remotely access the organization's network and systems.
INFOSEC20	Router and switch security	Defining the minimum configuration requirement for routers and switches within the corporate network.
INFOSEC21	Security response plan	Defining a set of requirements that all business units need to maintain for a security response plan
INFOSEC22	Server security	Defining a baseline configuration for internal and cloud servers within the organizational network.
INFOSEC23	Software installation	Defining a set of requirements required for installed software within the organization.
INFOSEC24	Technology equipment disposal	Defining a process for the disposal of technology equipment after its end of life.
INFOSEC25	Web application security	Defining a set of requirements required for web applications consumed by the organization.
INFOSEC26	Wireless communication	Defining a set of requirements to secure and protect mobile devices when connecting to the corporate network.
INFOSEC27	Wireless communication standard	Defining a standard protocol for mobile devices when connecting to the corporate network through wireless.
INFOSEC28	Workstation security	Defining a baseline security configuration for workstations within the organization.

Title: **Acceptable Encryption Policy**	P&P #: **INFOSEC01**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC01 - Acceptable Encryption Policy

1. Purpose

The purpose of this policy is to define a standard for the use of acceptable encryption mechanism within the organization.

2. Scope

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that PCI-compliance is followed.

3. Policy

3.1. Policy

The encryption algorithms should utilize AES as it is proven to have the strongest encryption capabilities compared to DES or Blowfish (Cruz, Fernandez, Palicpic, Uyehara & Tayuan, 2018).

Table 2 – Permitted encryption methods

Algorithm	Key Length
ECDSA	P-256
RSA	2048
LDWM	SHA256

The AES encryption methodology is continuously being revisited whereby new instructions are added to the current cryptographic method, known as AES-NI and utilizing up to 256 keys (Faz-Hernandez, López & De Oliveira, 2018). The utilization of AES-256 and fingerprinting ensures that the contents of the file is decrypted only from specific machines who have the necessary private key.

3.2. Key agreement, authentication and storage

- Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).
- End points must be authenticated prior to the exchange or derivation of session keys.
- Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.
- All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.
- All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.
- Cryptographic keys must be generated and stored in a secure manner.

4. Policy compliance

4.1. 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.

4.2. Exceptions

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

4.3. Non-Compliance

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

Title: **Acceptable Use Policy**	P&P #: **INFOSEC02**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC02 - Acceptable Use Policy

1. Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>'s established culture of openness, trust and integrity. InfoSec is committed to protecting <Company Name>'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, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations

Effective security is a team effort involving the participation and support of every <Company Name> 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.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct <Company Name> business or interact with internal networks and business systems, whether owned or leased by <Company Name>, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at <Company Name> and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with <Company Name> 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, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

4. Policy

4.1. General use and ownership

- <Company Name> proprietary information stored on electronic and computing devices whether owned or leased by <Company Name>, the employee or a third party, remains the sole property of <Company Name>. You must ensure that proprietary information is protected in accordance with policies INFOSEC04 (Clean desk), INFOSEC16 (Password construction), INFOSEC17 (Password protection) and INFOSEC28 (Workstation security).
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of <Company Name> proprietary information.
- You may access, use or share <Company Name> 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 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 <Company Name> may monitor equipment, systems and network traffic at any time, per INFOSEC11 (Information logging standard).
- <Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with INFOSEC13 (Minimum Access).
- System level and user level passwords must comply with the INFOSEC16 (Password construction) and INFOSEC17 (Password protection). 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 screensaver 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 <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of 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 <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-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.

The following activities are strictly 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 <Company Name>.
- 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 <Company Name> or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting <Company Name> 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 export of any material that is in question.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password 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 <Company Name> 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 <Company Name> 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, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec 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 <Company Name> 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, <Company Name> employees to parties outside <Company Name>.
- 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 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 <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

- Blogging by employees, whether using <Company Name>’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 <Company Name>’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>’s policy, is not detrimental to <Company Name>’s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>’s systems is also subject to monitoring.
- <Company Name>’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>’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 <Company Name> and/or any of its employees.
- Employees may also not attribute personal statements, opinions or beliefs to <Company Name> 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 <Company Name>. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, <Company Name>’s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1. 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.

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Bluetooth Baseline Requirements Policy**	P&P #: **INFOSEC03**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC03 - Bluetooth Baseline Requirements Policy

1. Overview

Bluetooth enabled devices are exploding on the Internet at an astonishing rate. At the range of connectivity has increased substantially. Insecure Bluetooth connections can introduce a number of potential serious security issues. Hence, there is a need for a minimum standard for connecting Bluetooth enable devices.

2. Purpose

The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the <Company Name> network or <Company Name> owned devices. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential <Company Name> data.

3. Scope

This policy applies to any Bluetooth enabled device that is connected to <Company Name> network or owned devices.

4. Policy

4.1. Bluetooth version

- No Bluetooth Device shall be deployed on <Company Name> equipment that does not meet a minimum of Bluetooth v4.1 specifications (Padgette et al., 2017) without written authorization from the InfoSec Team. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

4.2. Pins and Pairing

- When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where you PIN can be compromised.
- If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, you must refuse the pairing request and report it to InfoSec, through the Help Desk, immediately.

4.3. Device Security Settings

- All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
- Use a minimum PIN length of 8. A longer PIN provides more security.
- Switch the Bluetooth device to use the hidden mode (non-discoverable)
- Only activate Bluetooth only when it is needed.
- Ensure device firmware is up-to-date.

4.4. Security Audits

- The InfoSec Team may perform random audits to ensure compliancy with this policy. In the process of performing such audits, InfoSec Team members shall not eavesdrop on any phone conversation.

4.5. Unauthorized Use

The following is a list of unauthorized uses of <Company Name>-owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
- Using <Company Name>-owned Bluetooth equipment on non-<Company Name>-owned Bluetooth enabled devices.

- Unauthorized modification of Bluetooth devices for any purpose.

4.6. User Responsibilities

- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth mode must be turned off when not in use.
- PII and/or <Company Name> Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.
- Bluetooth users must only access <Company Name> information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to InfoSec.

5. Policy Compliance

5.1. 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.

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Clean Desk Policy**	P&P #: **INFOSEC04**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC04 - Clean Desk Policy

1. Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

2. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site.

3. Scope

This policy applies to all <Company Name> employees and affiliates.

4. Policy

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the work day.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5. Policy Compliance

5.1. 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.

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Data Breach Response Policy**	P&P #: **INFOSEC05**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC05 - Data Breach Response Policy

1. Overview

This policy mandates that any individual who suspects that a theft, breach or exposure of <Company Name> Protected data or <Company Name> Sensitive data has occurred must immediately provide a description of what occurred via e-mail to InfoSec@<Company Name>.com, by calling 555-1212, or through the use of the help desk reporting web page at http://ITSM.<Company Name>.com. This e-mail address, phone number, and web page are monitored by the <Company Name>'s Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the InfoSec team will follow the appropriate procedure in place.

2. Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

<Company Name> Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how <Company Name>'s established culture of openness, trust and integrity should respond to such activity. <Company Name> Information Security is

committed to protecting <Company Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

3. Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or financial details.

4. Policy

As soon as a theft, data breach or exposure containing <Company Name> Protected data or <Company Name> Sensitive data is identified, the process of removing all access to that resource will begin. The Information Security Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Department
- Finance (if applicable)
- Legal
- Communications
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved
- Additional individuals as deemed necessary by the Information Security Director

The Information Security Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

4.1. Engagement of Private Forensic Investigators and Cyber security partners

As recommended by PCI, a private forensic investigator will be engaged (PCI Security Standards, 2021), together with a cybersecurity partner to determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

4.2. Develop a communication plan.

Work with <Company Name> communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

5. Policy Compliance

5.1. Compliance Measurement

The InfoSec team will verify compliance to this policy through feedback from the policy owner.

5.2. Exceptions

Any exception to the policy must be approved by the Information Security Director.

5.3. Non-Compliance

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

Title: **Database Credentials Coding Policy**	P&P #: **INFOSEC06**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC06 - 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 very sensitive assets and be a springboard to wider compromise within the organization.

2. 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 <Company Name>'s networks.

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

3. Scope

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

4. Policy

4.1. General

In order to maintain the security of <Company Name>'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. Database credentials must not be stored in a location that can be accessed through a web server.

4.2. Storage of Data Base User Names and Passwords

- Database user names 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.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the INFOSEC16 (Password Construction Policy).

4.3. Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.
- 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 user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

4.4. Access to Database User Names and Passwords

- 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.
- Database passwords used by programs are system-level passwords as defined by the INFOSEC16 (Password Construction Policy).
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the INFOSEC16 (Password Construction Policy). This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

4.5. Coding Techniques for implementing this policy

- Applications and microservices should utilize secrets and authentication tools such as *Auth0*.

5. Policy Compliance

5.1. 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.

5.2. Exceptions

Any exception to the policy must be approved by the Information Security Director.

5.3. Non-Compliance

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

6. Related Standards, Policies and Processes

- INFOSEC 16 - Password Construction Policy
- INFOSEC 17 – Password Protection Policy

Title: **Digital Signature Acceptance Policy**	P&P #: **INFOSEC07**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC07 - Digital Signature Acceptance Policy

1. Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in <Company Name> electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

2. Scope

This policy applies to all <Company Name> employees, contractors, and other agents conducting <Company Name> business with a <Company Name>-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-<Company Name> affiliated persons or organizations.

3. Policy

- A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted on the site of the Chief Financial Officer (CFO) on the organization's intranet: intranet.cfo.<Company Name>.com.
- The CFO's office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.
- Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

3.1. Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

3.2. Signer Responsibilities

- Signers must obtain a signing key pair from <Company Name identity management group>. This key pair will be generated using <Company Name>'s Public Key Infrastructure (PKI) and the public key will be signed by the <Company Name>'s Certificate Authority (CA), <CA Name>.
- Signers must sign documents and correspondence using software approved by <Company Name> IT organization.
- Signers must protect their private key and keep it secret.
- If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact <Company Name> Identity Management Group immediately to have the signer's digital key pair revoked.

3.3. Recipient Responsibilities

- Recipients must read documents and correspondence using software approved by <Company Name> IT department.
- Recipients must verify that the signer's public key was signed by the <Company Name>'s Certificate Authority (CA), <CA Name>, by viewing the details about the signed key using the software they are using to read the document or correspondence.

- If the signer’s digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.
- If a recipient believes that a digital signature has been abused, the recipient must report the recipient’s concern to <Company Name> Identity Management Group.

4. Policy Compliance

4.1. 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.

4.2. Exceptions

Any exception to the policy must be approved by the Information Security Director.

4.3. Non-Compliance

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

Title: **Disaster Recovery Plan Policy**	P&P #: **INFOSEC08**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC08 - Disaster Recovery Plan Policy

1. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives <Company Name> a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered as a Disaster. The Disaster Recovery Plan is often part of the Business Continuity Plan.

2. Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by <Company Name> that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up to date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

4. Policy

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Tabletop exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

Any exception to the policy must be approved by the Information Security Director.

5.3. Non-Compliance

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

Title: **End User Encryption Key Protection Policy**	P&P #: **INFOSEC09**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC09 - End User Encryption Key Protection Policy

1. Overview

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys use to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

2. Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

3. Scope

This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

- encryption keys issued by <Company Name>
- encryption keys used for <Company Name> business
- encryption keys used to protect data owned by <Company Name>

The public keys contained in digital certificates are specifically exempted from this policy.

4. Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

4.1. Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in <Company Name>'s *Acceptable Encryption Policy.* If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key. Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

4.2. Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

4.3. <Company Name>'s Public Key Infrastructure (PKI) Keys

The public-private key pairs used by the <Company Name>'s public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents the Infosec

Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with <Company Name> policies.

Access to the private keys stored on a <Company Name>issued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

4.4. Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the requirements for protecting the private keys are the same as those for private keys associated with <Company Name's> PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.

The Infosec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with <Company Name> *Password Policy*. Infosec representatives will store and protect the escrowed keys as described in the <Company Name> *Certificate Practice Statement Policy.*

4.5. Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user’s web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser’s certificate store where the only protection is the password on the browser’s certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

4.6. PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user’s key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

4.7. Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in <Company Name>’s *Physical Security policy,* when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user’s computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

4.8. Personal Identification Numbers (PINs), Passwords and Passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in <Company Name>’s *Password Policy.*

4.9. Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to The Infosec Team. Infosec personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

Any exception to the policy must be approved by the Information Security Director.

5.3. Non-Compliance

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

6. Related Standards, Policies and Processes

- INFOSEC01– Acceptable Encryption Policy
- INFOSEC16 – Password Construction Policy
- INFOSEC17 – Password Protection Policy

Title: **Ethics Policy**	P&P #: **INFOSEC10**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC10 - Ethics Policy

1. Overview

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

2. 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 <Company Name> employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

3. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties.

4. Policy

4.1. Executive Commitment to Ethics

- Senior leaders and executives within <Company Name> 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 interests regard their position within <Company Name>.

4.2. Employee Commitment to Ethics

- <Company Name> 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 ethics value.
- Employees must disclose any conflict of interests regard their position within <Company Name>.
- Employees will help <Company Name> 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 <Company Name> policies?
  - Does the behavior reflect <Company Name> 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 <Company Name> if all employees did it?

4.3. Company Awareness

- Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- <Company Name> will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. Maintaining Ethical Practices

- <Company Name> will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.
- Employees at <Company Name> should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
- <Company Name> 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 to Ethics Policy on an annual basis.

4.5. Unethical Behavior

- <Company Name> will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
- <Company Name> 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.

- <Company Name> will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.
- <Company Name> employees will not use corporate assets or business relationships for personal use or gain.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

None

5.3. Non-Compliance

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

Title: **Information Logging Standard Policy**	P&P #: **INFOSEC11**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC11 - Information Logging Standard Policy

1. Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

2. Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function. The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

3. Scope

This policy applies to all production systems on <Company Name> Network.

4. Policy

4.1. General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
- Who or what performed the activity, including where or on what system the activity was performed from (subject)?

- What the activity was performed on (object)?
- When was the activity performed?
- What tool(s) was the activity was performed with?
- What was the status (such as success vs. failure), outcome, or result of the activity?

4.2. Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

- Create, read, update, or delete confidential information, including confidential authentication information such as passwords.
- Initiate a network connection.
- Accept a network connection.
- User authentication and authorization for activities covered in #1 or #2 such as user login and logout.
- Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes.
- System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes.
- Application process startup, shutdown, or restart.
- Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault.

- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3. Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

- Type of action – examples include authorize, create, read, update, delete, and accept network connection.
- Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
- Identifiers (as many as available) for the subject requesting the action – examples include username, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
- Before and after values when action involves updating a data element, if feasible.
- Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
- Whether the action was allowed or denied by access-control mechanisms.
- Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4. Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

- Microsoft Windows Event Logs collected by a centralized log management system.
- Logs in a well-documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system.
- Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document.
- Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Lab Security Policy**	P&P #: **INFOSEC12**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC12 - Lab Security Policy

1. Purpose

This policy establishes the information security requirements to help manage and safeguard lab resources and <Company Name> networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

2. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at <Company Name> and its subsidiaries must adhere to this policy. This policy applies to <Company Name> owned and managed labs, including labs outside the corporate network, referred to as DMZ in this policy.

3. Policy

3.1. General Requirements

- Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up to date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.
- Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard <Company Name> from security vulnerabilities.

- Lab managers are responsible for the lab's compliance with all <Company Name> security policies.
- The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.
- All user passwords must comply with <Company Name>'s *Password Policy*.
- Individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months).
- PC-based lab computers must have <Company Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.
- Any activities with the intention to create and/or distribute malicious programs into <Company Name>'s networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.
- No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

- In accordance with *the Data Classification Policy*, information that is marked as <Company Name> Highly Confidential or <Company Name> Restricted is prohibited on lab equipment.
- Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*.
- InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

3.2. Internal Lab Security Requirements

- The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.
- The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.
- The Network Support Organization must record all lab IP addresses, which are routed within <Company Name> networks, in Enterprise Address Management database along with current contact information for that lab.
- Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.
- All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

- Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.
- Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-<Company Name> networks. These activities must be restricted within the lab.
- Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.
- InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.
- Lab owned gateway devices are required to comply with all <Company Name> product security advisories and must authenticate against the Corporate Authentication servers.
- The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with <Company Name>'s *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.
- In labs where non-<Company Name> personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no <Company Name> confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network

only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

- Lab networks with external connections are prohibited from connecting to the corporate production network or other internal networks through a direct connection, wireless connection, or other computing equipment.

3.3. DMZ Lab Security Requirements

- New DMZ labs require a business justification and VP-level approval from the business unit. Changes to the connectivity or purpose of an existing DMZ lab must be reviewed and approved by the InfoSec Team.
- DMZ labs must be in a physically separate room, cage, or secured lockable rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.
- DMZ lab POCs must maintain network devices deployed in the DMZ lab up to the network support organization point of demarcation.
- DMZ labs must not connect to corporate internal networks, either directly, logically (for example, IPSEC tunnel), through a wireless connection, or multi-homed machine.
- An approved network support organization must maintain a firewall device between the DMZ lab and the Internet. Firewall devices must be configured based on least privilege access principles and the DMZ lab business requirements. Original firewall configurations and subsequent changes must be reviewed and approved by the InfoSec Team. All traffic between the DMZ lab and the Internet must go through the approved firewall. Cross-connections that bypass the firewall device are strictly prohibited.

- All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
- Operating systems of all hosts internal to the DMZ lab running Internet Services must be configured to the secure host installation and configuration standards published the InfoSec Team.
- Remote administration must be performed over secure channels (for example, encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.
- DMZ lab devices must not be an open proxy to the Internet.
- The Network Support Organization and InfoSec reserve the right to interrupt lab connections if a security concern exists.

4. Policy Compliance

4.1. Compliance Measurement

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

4.2. Exceptions

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

4.3. Non-Compliance

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

Title: **Minimum Access Policy**	P&P #: **INFOSEC13**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC13 - Minimum Access Policy

1. Overview

<Company Name> gives minimum amount of access on files and directories such as of personally identifiable information all employees, contractors, consultants, temporary and other workers. This policy also details the minimum conditions that the computers need to meet, in order to be allowed on to the network.

2. Purpose

The purpose of this policy is to make sure that all employees, contractors, consultants, temporary and other workers are aware of the minimum access to sensitive information such as personally identifiable information and minimum conditions for computer access.

3. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers of <Company Name>.

4. Policy

4.1. File system Security

<Company Name>. gives the minimum amount of access on files and directories as possible. No unauthorized user should attempt to access files of sensitive nature, which will be known because of the password protection or the restricted profile. The concept of minimum access extends beyond the scope of file systems into almost all realms of security.

4.2. Computer connection to network

Computers need to meet minimum conditions in order to connect to <Company Name> WiFi and network resources. They must have at least updated antivirus and updated software patch level. These policies will be enforced by means of Network Access Control systems and by means of automated compliance-checking processes that scan the network to obtain a snapshot of the compliance level of the computers. You are responsible for the security and appropriate use of <Company Name> network resources under your control.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **PCI Compliancy Policy**	P&P #: **INFOSEC14**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC14 - PCI Compliancy Policy

1. Purpose

The purpose of this policy is to establish a security posture for the interaction of cardholder data and reduce the burden of the implementation and management of PCI of applicable controls required by the most current version of the Payment Card Industry Data Security Standard (PCI DSS).

Unless otherwise provisioned, documented, or communicated, this document establishes policy as it relates to the storage, processing, or transmission of cardholder data within <Company Name>.

2. Scope

This document applies to all employees, contractors, and third-party entities that store, process, transmit cardholder data, or otherwise interact with cardholder data which is processed against any transaction where <Company Name> owns or is responsible for the associated merchant ID (MID). Furthermore, this policy applies to all devices that are used for the physical capture of cardholder data used to capture those transactions.

3. Policy

3.1. Transaction Processing

- All payment processing must be facilitated through a validated PCI P2PE solution approved and listed by the PCI Security Standards Council (SSC). No other forms of transaction processing will be permitted or approved.
- <Company Name> may not receive or transmit cardholder data electronically outside of a validated P2PE solution.

3.2. PCI P2PE Devices

- All devices must be deployed in accordance with the vendor provided P2PE Implementation Guide.
- Care, custody, and control must be applied to each device used to interact with cardholder data. These processes must include, but are not limited to, the following:
    - Inventory management
        - A formal inventory of all P2PE payment devices must be maintained.
        - A formal process to maintain this list must be implemented. This will include asset management of devices in production, inventory, reallocation, and decommissioning.
        - A formal inspection process must be implemented to ensure that there has not been any unauthorized substitution.
        - A formal list of each device must be maintained. This list will include but is not limited to:
            - Make and model of device
            - Location of device
            - Unique identifier
    - Device security
        - Devices must be inspected on a monthly basis. This inspection must be sufficient to identify a tampered device.

3.3. Employee Training

Individuals must receive training sufficient to:

- Identify any payment device which has been tamped with.
- Be aware of suspicious behavior around payment devices.

- Be aware of devices which have been tamped with or substituted.
- Verify the identity of any individual claiming to provide repair or maintenance services.
- Not install, replace, or return devices without formal verification and approval by Director of Information Security.
- Report any suspicious behavior to InfoSec team.
- Follow formal processes for inspection of any payment device used for cardholder data.
- Maintain the established frequency of inspection of payment devices.

3.4. Cardholder Data Storage

- Storage of electronic/digital cardholder data is prohibited, unless required for documented legal reasons.
- Storage of sensitive authentication data after authorization is prohibited.
- Storage of physical print media is permitted, given the following requirements are met:
    - A formal data retention policy must exist that defines the data that is retained, and the purpose of the retention. This retention must be defined with specific legal and/or business reasons.
    - Physical print media containing cardholder data may not be stored for longer than its defined retention period.
    - There must be a formal process, executed quarterly, to identify any data which has exceeded the retention period.
    - In the event cardholder data has been identified as exceeding its retention period, a formal process must be implemented to securely dispose of it. Destroyed data should not be able to be recovered or reconstructed.

- Storage of physical print media must be secured from any unauthorized access.

4. Policy Compliance

4.1. Compliance Measurement

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

4.2. Exceptions

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

4.3. Non-Compliance

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

Title: **Pandemic Response Planning Policy**	P&P #: **INFOSEC15**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC15 - Pandemic Response Planning Policy

1. Overview

This policy is intended for companies that do not meet the definition of critical infrastructure as defined by the US Federal Government. This type of organization may be requested by public health officials to close their offices to non-essential personnel or completely during a pandemic to lower the immediate risk and limit the spread of the disease. Many companies would run out of cash and be forced to go out of business after several weeks of everyone not working. Therefore, developing a response plan in advance that addresses who can work remotely, how they will work and identifies what other issues may be faced will help the organization survive at a time when most people will be concerned about themselves and their families.

Disasters typically happen in one geographic area. A hurricane or earthquake can cause massive damage in one area, yet the worst damage is usually contained within a few hundred miles. A global pandemic, such as the 1918 influenza outbreak which infected 1/3 of the world’s population, cannot be dealt with by failing over to a backup data center. Therefore, additional planning steps for IT architecture, situational awareness, employee training and other preparations are required.

2. Purpose

This document directs planning, preparation and exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process. The objective is to address the reality that pandemic events can create personnel and technology issues outside the scope of the traditional Disaster Recovery/Business Continuity Planning process as potentially some if not the entire workforce may be unable to come to work for health or personal reasons.

3. Scope

The planning process will include personnel involved in the business continuity and disaster recovery process, enterprise architects and senior management of <Company Name>. During the implementation of the plan, all employees and contractors will need to undergo training before and during a pandemic disease outbreak.

4. Policy

<Company Name> will authorize, develop and maintain a Pandemic Response Plan addressing the following areas:

- The Pandemic Response Plan leadership will be identified as a small team which will oversee the creation and updates of the plan. The leadership will also be responsible for developing internal expertise on the transmission of diseases and other areas such as second wave phenomenon to guide planning and response efforts. However, as with any other critical position, the leadership must have trained alternates that can execute the plan should the leadership become unavailable due to illness.
- The creation of a communications plan before and during an outbreak that accounts for congested telecommunications services.
- An alert system based on monitoring of World Health Organization (WHO), the Centers for Disease Control (CDC) and other Federal, State and Local sources of information on the risk of a pandemic disease outbreak.
- A predefined set of emergency policies that will preempt normal <Company Name> policies for the duration of a declared pandemic. These emergency policies are to be organized into different levels of response that match the

level of business disruption expected from a possible pandemic disease outbreak within the community. These policies should address all tasks critical to the continuation of the company including:

  - How people will be paid
  - Where people will work – including staying home with or bringing kids to work
  - How people will accomplish their tasks if they cannot get to the office
  - What work will be suspended during the pandemic
  - Communication plan and cadence throughout the pandemic
  - Alternate means to communicate during the pandemic
  - What operational procedures may need to be altered, amended, or suspended, such as those over facilities, visitors, and non-essential activities and events

- A set of indicators to management that will aid them in selecting an appropriate level of response bringing into effect the related policies discussed in section 4.4—for the organization. There should be a graduated level of response related to the WHO pandemic alert level or other authoritative indicators of a disease outbreak.
- An employee training process covering personal protection including:
  - Identifying and broadly communicating the symptoms of exposure
  - The concept of disease clusters in daycares, schools or other large gatherings
  - Basic prevention - limiting contact closer than 6 feet, cover your cough, hand washing
  - When to stay home along with encouragement to do so
  - Avoiding travel to all areas with high infection rates

- A process for the identification of employees with first responders or medical personnel in their household. These people, along with single parents, have a higher likelihood of unavailability due to illness or childcare issues.
- A process to identify key personnel for each critical business function and transition their duties to others in the event they become ill or unable to perform their respective duties.
- A list of supplies to be kept on hand or pre-contracted for supply, such as face masks, hand sanitizer, fuel, food and water.
- IT related issues:
    - Ensure enterprise architects are including pandemic contingency in planning
    - Verification of the ability for significantly increased telecommuting including bandwidth, VPN concentrator capacity/licensing, ability to offer voice over IP and laptop/remote desktop availability
    - Increased use of virtual meeting tools that facilitate video conference and desktop sharing capabilities
    - Identify what tasks cannot be done remotely
    - Pre-negotiated arrangements with key vendors in the event current licensing will not meet this change in work force habits
    - Determine if any IT colleagues need to remain onsite to support critical operations
    - Plan for how customers will interact with the organization in different ways
    - Expectations concerning printing work documents on personal printers
    - Expectations about sending work emails and documents to personal email accounts

- The creation of exercises to test the plan in advance.
- Performing a retrospective review to identify and solve for issues encountered in the test.
- The process and frequency of plan updates and review at least annually with appropriate approvals or sign-off from organizational leadership or oversight.
- Guidance for auditors indicating that any review of the business continuity plan or enterprise architecture should assess whether they appropriately address the <Company Name> Pandemic Response Plan.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Password Construction Policy**	P&P #: **INFOSEC16**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC16 - Password Construction Policy

1. Overview

A password policy is a set of rules designed to increase computer security by encouraging users to employ strong passwords and use them properly. The purpose of this policy is to assist <Company Name. and all subsidiaries in understanding the activities performed as part of creating, maintaining and changing of passwords that is used and/or operated by <Company Name>, and therefore to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. The scope of the policy includes all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system within the organization's facility and/or has access to the <Company Name> network. Passwords are an important aspect of computer security. They are the primary authentication method for the IT resources and are currently employed as the basis authentication method. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of <Company Name>'s entire corporate network, and thus a security breach, loss or exposure of potentially sensitive data, system compromise and compromise of other network systems. All <Company Name> users (including contractors, consultants, resellers, vendors, and all other individual and groups who have been granted access to <Company Name>'s network, with access to <Company Name> network) are responsible for taking the appropriate steps, as outlined in this policy, to select and secure their passwords.

2. Purpose

The purpose of this policy is to provide best practices for the created of strong passwords.

3. 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, screen saver protection, voicemail, and local router logins.

4. Policy

4.1. System (Administrators) Level Passwords

- All system level passwords (including root, admin and others) must be changed on a regular basis.
- User accounts that have system-level privileges granted through group memberships or programs such as "SUDO" should have a unique password from all other accounts held by that user, unless this is required for the execution of tasks.
- Application Developers should ensure that their programs support:
  - authentication of users.
  - do not store passwords in clear text or in an easily reversible format (one time passwords authentication or private/public key system with a strong passphrase).
  - 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.
- System administrators and computer support staff who configure new systems and set up services are to ensure that all password settings are changed from their default settings before moving platforms into production, if such changes are permitted by vendor.

- Shared administrator and super-user (global) passwords are not to be used on production systems except where passwords are hard coded into applications, as long as this is permitted by vendor. It is strongly recommended that this rule is also applied to development and research systems.
- Administrators and IT support staff are to be allocated secondary accounts which have the appropriate rights and privileges to enable them to support the systems and services for which they have a responsibility.
- <Company Name> will not necessarily configure its systems to enforce password complexity but users are required to choose strong passwords.

4.2. User Level (Staff) Passwords

- Each employee must protect all passwords and must not distribute them in any written or electronic form. Passwords should not be stored in any file on any computer system; including portable devices, unless proper encryption is in place.
- Employees should be notified of how to construct a secure strong password. Passwords must not be easy to guess or the same as username or as used in other systems' accounts, being inside or outside <Company Name>.
- It is recommended that all users' passwords must be changed every 60 days.
- Do not use the "Remember Password" feature of applications.
- If an account or password is suspected to have been compromised, this needs to be reported immediately to the IT Helpdesk.
- Wherever possible, account lockout thresholds must be activated when more than five password login attempts fail, with login failures being recorded.
- Each employee must be assigned a password complimenting his/her username for access identification on any <Company Name> systems.
- Usernames and passwords must never be shared.

- Passwords must be re-entered if employees leave their workstations, even for a short while. Thus, when an employee leaves his/her desk s/he must lock his/her computer.
- If passwords are forgotten and need to be changed, users should ask assistance from the IT Helpdesk.
- Password changes should be unique from previous passwords on systems that support this feature.
- When a request for a username is requested, the ticket should also include 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 this policy.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- A user needs to immediately request a change in password if there is any doubt that a password has been compromised.

4.3. Password Construction Guidelines

Passwords are used for a variety of purposes at <Company Name>. Anyone, who has or is responsible for an account on any system within the organization's facility and/or has access to the <Company Name> LTD network, 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). All real words are easy to guess.

- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, favorite football teams, favorite sports teams, partners, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words <Company Name>, <Company Name>ltd, <Company Name>cable or any derivation.
- Birthdays and other personal information such as addresses, phone numbers, mobile numbers, personal cars, personal cars' registration,
- Something that is easy to guess from watching like QWERTY, 123456, 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:

- Minimum password length: ***8 characters***
- Maximum password age: ***60 days***
- Minimum password age: ***15 days***
- Password history: ***3 passwords remembered***
- Password complexity: ***Alpha-numeric with numbers and special characters***

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

	Policy and Procedure
Title: **Password Protection Policy**	P&P #: **INFOSEC17**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC17 - Password Protection Policy

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This guideline provides best practices for creating secure passwords.

2. Purpose

The purpose of this policy is to provide best practices for the protection of passwords.

3. 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, screen saver protection, voicemail, and local router logins.

4. Policy

- Do not use the same password for <Company Name>accounts as for other non-<Company Name>access.
- When possible, don't use the same password for various company access needs.
- Select a separate password to be used for a Microsoft windows' account and a non-Microsoft operating system account.
- Do not share any of the passwords with anyone, including relatives, supervisors, senior management, and IT services, amongst others.

- All passwords are to be treated as sensitive, confidential <Company Name>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, or through private chats, or through social engineering
    - Don't reveal a password to your colleague’s even while on vacation
    - Don’t leave password blank
    - 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 reuse or recycle a password; i.e. new passwords must not bear any relation to the old.
    - Don’t let other people watch you key your password in, known also as shoulder surfing
- If someone demands a password, refer them to this policy or have them call someone in the IT Helpdesk.
- Passwords are secret and users are responsible for protecting their own passwords. Also, it is important to note that computers that are left unattended and logged in gives anyone access to information accessible to the authorized user. If a computer is left unattended, it should be locked through the use of a password access hot-key, or password protected screen saver. Users must log off the network when finished working.
- The InfoSec team may introduce a password manager such as *1Password* or *Dashlane* to facilitate password storage for user and systems.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Remote Access Policy**	P&P #: **INFOSEC18**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC18 - Remote Access Policy

1. Overview

Remote access to the corporate network is essential to maintain the organization’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 <Company Name>, users must mitigate external risks to the best of their abilities.

2. Purpose

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

3. Scope

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

4. Policy

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

General access to the Internet for recreational use through the <Company Name> network is strictly limited to <Company Name> employees, contractors, vendors and agents (hereafter referred to as “Authorized Users”). When accessing the <Company Name> network from a personal computer, Authorized Users are responsible for preventing access to any <Company Name> computer resources or data by non-Authorized Users. Performance of illegal activities through the <Company Name> 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 <Company Name> networks to access the Internet for outside business interests.

For additional information regarding <Company Name>'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 (company URL).

4.1. Requirements

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases. For further information see the INFOSEC01 (Acceptable Encryption Policy) and INFOSEC16 (Password Construction Policy).
- Authorized Users shall protect their login and password, even from family members.

- While using a <Company Name>-owned computer to remotely connect to <Company Name>'s corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of 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 <Company Name> business must be approved in advance by InfoSec and the appropriate business unit manager.
- All hosts that are connected to <Company Name> internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third-Party Agreement*.
- Personal equipment used to connect to <Company Name>'s networks must meet the requirements of <Company Name>-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to <Company Name> Networks*.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Remote Access Tools Policy**	P&P #: **INFOSEC19**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC19 - Remote Access Tools Policy

1. Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the <Company Name> 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 <Company Name> computer systems.

2. Purpose

This policy defines the requirements for remote access tools used at <Company Name>.

3. Scope

This policy applies to all remote access where either end of the communication terminates at a <Company Name> computer assets.

4. Policy

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

4.1. Remote Access Tools

<Company Name> provides mechanisms to collaborate between internal users, with external partners, and from non-<Company Name> systems. The approved software list can be obtained from <link-to-approved-remote-access-software-list>. 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:

- All remote access tools or systems that allow communication to <Company Name> 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.
- 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. The remote access tool must mutually authenticate both ends of the session.
- Remote access tools must support the <Company Name> application layer proxy rather than direct connections through the perimeter firewall(s).
- Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the <Company Name> network encryption protocols policy.
- All <Company Name> 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 <Company Name> procurement process, and the information technology group must approve the purchase.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Router and Switch Security Policy**	P&P #: **INFOSEC20**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC20 - Router and Switch Security Policy

1. 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 <Company Name>.

2. Scope

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

3. 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 authentication.
- 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 running on router
  - <Company Name> 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:
  - <Company Name> 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

4. Policy Compliance

4.1. Compliance Measurement

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

4.2. Exceptions

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

4.3. Non-Compliance

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

Title: **Security Response Plan Policy**	P&P #: **INFOSEC21**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC21 - Security Response Plan Policy

1. Overview

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

2. Purpose

The purpose of this policy is to establish the requirement that all business units supported by the Infosec team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

3. Scope

This policy applies any established and defined business unity or entity within the <Company Name>.

4. Policy

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with the Infosec Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the <organizational information security unit> in the development and maintenance of a Security Response Plan.

4.1. Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2. Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

4.3. Triage

The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4. Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5. Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5. Policy Compliance

5.1. Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2. Exceptions

Any exception to the policy must be approved by the Infosec team in advance and have a written record.

5.3. Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP

Title: **Server Security Policy**	P&P #: **INFOSEC22**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC22 - 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.

2. 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 <Company Name>. Effective implementation of this policy will minimize unauthorized access to <Company Name> proprietary information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at <Company Name> must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by <Company Name> or registered under a <Company Name>-owned internal network domain. This policy specifies requirements for equipment on the internal <Company Name> network.

4. Policy

4.1. General Requirements

All internal servers deployed at <Company Name> 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 InfoSec. 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

4.2. Configuration Requirements

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- 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.
- 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.

- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
- 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).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3. Monitoring

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.

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.

5. Policy Compliance

5.1. Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2. Exceptions

Any exception to the policy must be approved by the Infosec team in advance and have a written record.

5.3. Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP

Title: **Software Installation Policy**	P&P #: **INFOSEC23**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC23 - 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.

2. Purpose

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

3. Scope

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

4. Policy

- Employees may not install software on <Company Name's> computing devices operated within the <Company Name> network.

- 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.
- 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.
- The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Technology Equipment Disposal Policy**	P&P #: **INFOSEC24**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC24 - Technology Equipment Disposal Policy

1. Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of <Company Name> data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

2. Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by <Company Name>.

3. Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within <Company Name> including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials. All <Company Name> employees and affiliates must comply with this policy.

4. Policy

4.1. Technology Equipment Disposal

- When Technology assets have reached the end of their useful life they should be sent to the <Equipment Disposal Team> office for proper disposal.
- The <Equipment Disposal Team> will securely erase all storage mediums in accordance with current industry best practices.
- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.
- No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).
- No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around <Company Name>. These can be used to dispose of equipment. The <Equipment Disposal Team> will properly remove all data prior to final disposal.
- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

- The <Equipment Disposal Team> will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

4.2. Employee Purchase of Disposed Equipment

- Equipment, which is working, but reached the end of its useful life to <Company Name>, will be made available for purchase by employees.
- A lottery system will be used to determine who has the opportunity to purchase available equipment.
- All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.
- Finance and Information Technology will determine an appropriate cost for each item.
- All purchases are final. No warranty or support will be provided with any equipment sold.
- Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information
- Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.
- Prior to leaving <Company Name> premises, all equipment must be removed from the Information Technology inventory system.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Web Application Security Policy**	P&P #: **INFOSEC25**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC25 - Web Application Security Policy

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.

2. Purpose

The purpose of this policy is to define web application security assessments within <Company Name>. Web application assessments are performed to identify potential or realized weaknesses as a result 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 <Company Name> services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. 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 <Company Name>.

All web application security assessments will be performed by delegated security personnel either employed or contracted by <Company Name>. All findings are considered confidential and are to be distributed to persons on a “need to know” basis. Distribution of any findings outside of <Company Name> is strictly 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.

4. Policy

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

- 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.
- Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
- Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- 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 carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

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.

- 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.
- 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 will limit exposure.
- Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

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

- 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 any and all discovered.
- 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.
- Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. 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.

Title: **Wireless Communication Policy**	P&P #: **INFOSEC26**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC26 - Wireless Communication Policy

1. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

2. Purpose

The purpose of this policy is to secure and protect the information assets owned by <Company Name>. <Company Name> provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. <Company Name> grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to <Company Name> network. Only **those** wireless infrastructure devices that meet the standards **specified in** this policy or are granted an exception by the Information Security Department are approved for connectivity to a <Company Name> network.

3. Scope

All employees, contractors, consultants, temporary and other workers at <Company Name>, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of <Company Name> must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a <Company Name> network or reside on a <Company Name> site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4. Policy

4.1. General Requirements

All wireless infrastructure devices that reside at a <Company Name> site and connect to a <Company Name> network, or provide access to information classified as <Company Name> Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use <Company Name> approved authentication protocols and infrastructure.
- Use <Company Name> approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.2. Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to <Company Name> Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the <Company Name> network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the Lab Security Policy.
- Not interfere with wireless access deployments maintained by other support organizations.

4.3. Home Wireless Device Requirements

- Wireless infrastructure devices that provide direct access to the <Company Name> corporate network, must conform to the Home Wireless Device Requirements as detailed in INFOSEC27 (Wireless Communication Standard).
- Wireless infrastructure devices that fail to conform to INFOSEC27 (Wireless Communication Standard), must be installed in a manner that prohibits direct access to the <Company Name> corporate network. Access to the <Company Name> corporate network through this device must use standard remote access authentication.

5. Policy Compliance

5.1. Compliance Measurement

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

5.2. Exceptions

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

5.3. Non-Compliance

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

Title: **Wireless Communication Standard Policy**	P&P #: **INFOSEC27**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC27 - Wireless Communication Standard Policy

1. Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a <Company Name> network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity to a <Company Name> network. Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security (InfoSec) approved support organization. Lab network devices must comply with INFOSEC12 (Lab Security Policy).

2. Scope

All employees, contractors, consultants, temporary and other workers at <Company Name> and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of <Company Name>, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network. InfoSec must approve exceptions to this standard in advance.

3. Policy

3.1. General Requirements

All wireless infrastructure devices that connect to a <Company Name> network or provide access to <Company Name> Confidential, <Company Name> Highly Confidential, or <Company Name> Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

3.2. Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from <Company Name> production device SSID.
- Broadcast of lab device SSID must be disabled.

3.3. Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a <Company Name> network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

4. Policy Compliance

4.1. Compliance Measurement

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

4.2. Exceptions

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

4.3. Non-Compliance

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

Title: **Workstation Security Policy**	P&P #: **INFOSEC28**
Approval Date: **04-25-2021**	Review: **Annual**
Effective Date: **05-01-2021**	Version: **1**

INFOSEC28 - Workstation Security Policy

1. Purpose

The purpose of this policy is to provide guidance for workstation security for <Company Name> workstations in order to ensure the security of information on the workstation and information the workstation may have access to.

2. Scope

This policy applies to all <Company Name> employees, contractors, workforce members, vendors and agents with a <Company Name>-owned or personal-workstation connected to the <Company Name> network.

3. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including personal information and that access to sensitive information is restricted to authorized users. Workforce members using workstations shall consider the sensitivity of the information, including personal information that may be accessed and minimize the possibility of unauthorized access. <Company Name> will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users. Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with <Company Name> Password Policy.

- Complying with all applicable password policies and procedures. See INFOSEC17 (Password Protection Policy).
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including personal information on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the INFOSEC26 (Wireless Communication) policy.

4. Policy Compliance

4.1. Compliance Measurement

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

4.2. Exceptions

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

4.3. Non-Compliance

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

References

1Password. (2013). *Pricing for teams & businesses*. 1Password. Retrieved May 2, 2021 from https://1password.com/teams/pricing/

Bentley, J. M., & Ma, L. (2020). Testing perceptions of organizational apologies after a data breach crisis. *Public Relations Review, 46*(5), 101975. https://doi.org/10.1016/j.pubrev.2020.101975

Bischoff, P. (2019). Top 5 open-source network monitoring tools. Opensource.com. Retrieved March 20, 2021 from https://opensource.com/article/19/2/network-monitoring-tools

Cisco. (2018, September). *Cisco ASA Series CLI Configuration Guide, 9.0 - Configuring* QoS. Cisco. Retrieved March 20, 2021 from https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/conns_qos.html

Critchley, T. (2018, July 11*). GDPR and PCI DSS: How They Differ, How They're Similar and How to Comply with Both*. PaymentsJournal. Retrieved April 11, 2021 from https://www.paymentsjournal.com/gdpr-and-pci-dss/#:~:text=Reporting%20a%20Breach&text=The%20PCI%20DSS%2C%20on%20the,information%20with%20the%20card%20companies.

Cruz, J. J., Fernandez, R. D., Palicpic, C. M., Uyehara, D. L., & Tayuan, R. C. (2018). 'Pandora': A multi-encryption software. *Proceedings of the 2018 International Conference on Information Science and System - ICISS '18*. https://doi.org/10.1145/3209914.3209919

Faz-Hernandez, A., López, J., & De Oliveira A. K. D. S.. (2018). SoK: A performance evaluation of cryptographic instruction sets on modern architectures. *Proceedings of the 5th ACM on ASIA Public-Key Cryptography Workshop - APKC '18*. https://doi.org/10.1145/3197507.3197511

Fruhlinger, J. (2020, March 31). *12 top IDS/IPS tools*. CSO Online. Retrieved April 16, 2021 from https://www.csoonline.com/article/3532249/12-top-idsips-tools.html

Dynamic Insights. (2020). *Azure provides security to prevent ransomware attacks.* Archerpoint.com. Retrieved April 11, 2021 from https://www.archerpoint.com/blog/Posts/azure-provides-security-prevent-ransomware-attacks

Elastic. (2021). *SIEM on the Elastic Stack | Elastic Security*. (2021). Elastic. Retrieved March 20, 2021 from https://www.elastic.co/siem

ETCIO. (2020, September 16*). Several Microsoft SQL databases infected by new malware: Tencent*. ETCIO.com. Retrieved March 28, 2021 from https://cio.economictimes.indiatimes.com/news/digital-security/several-microsoft-sql-databases-infected-by-new-malware-tencent/78147074

HackerOne. (2021). *Security for Open Source Projects*. HackerOne. Retrieved May 2, 2021 from https://www.hackerone.com/company/open-source-community#:~:text=This%20fee%20is%20on%20top,hacker%20and%20%2450%20to%20HackerOne.

Hiscox. (2020). *Data exfiltration during ransomware attacks*. Hiscox.co.uk. Retrieved April 11, 2021 from https://www.hiscox.co.uk/sites/uk/files/documents/2020-07/20816-Data-exflitration-guide-final.pdf

IBM. (2018). *Monitoring QoS*. IBM. Retrieved March 20, 2021 from https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_71/rzak8/rzak8monitoring.htm

Kemme, B., Pedone, F., Alonso, G., Schiper, A., & Wiesmann, M. (2003). Using optimistic atomic broadcast in transaction processing systems. *IEEE Transactions on Knowledge and Data Engineering, 15*(4), 1018–1032. https://doi.org/10.1109/tkde.2003.1209016

Khan, M. T., DeBlasio, J., Voelker, G. M., Snoeren, A. C., Kanich, C., & Vallina-Rodriguez, N. (2018). An empirical analysis of the commercial VPN ecosystem. *In Proceedings of the Internet Measurement Conference 2018*. 443-456).

Kim, K., & Lee, M. (2018). SNMP-Based detection of VLAN Hopping attack risk. *Information Science and Applications 2018*, 267–272. https://doi.org/10.1007/978-981-13-1056-0_28

Malwarebytes. (2021). *Malwarebytes for Business*. Malwarebytes; Malwarebytes. Retrieved April 16, 2021 from https://www.malwarebytes.com/pricing/business/

Miller, R. (2011, May 4). *Sony's letter to Congress provides timeline for PlayStation Network breach, accuses Anonymous of incidental involvement.* The Verge. Retrieved April 2, 2021 from https://www.theverge.com/2011/5/4/2514919/sony-congress-playstation-network-anonymous

Mishra, D. (2020, March 19). *How to protect your VPN: Lessons from a DDoS attack Test*. Radware Blog. Retrieved March 20, 2021 from https://blog.radware.com/security/ddos/2020/03/how-to-protect-your-vpn-lessons-from-a-ddos-attack-test/

Mühlberg, B. (2020, March 30). *Ransomware attack hits FinTech company Finastra*. CPO Magazine. Retrieved April 11, 2021 from https://www.cpomagazine.com/cyber-security/ransomware-attack-hits-fintech-company-finastra/

Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2017). Guide to Bluetooth security. *NIST Special Publication, 800-121*(2). https://doi.org/10.6028/NIST.SP.800-121r2

Partida, D. (2020, September). *Financial industry targeted by ransomware hackers*. Socialnomics. Retrieved April 11, 2021 from https://socialnomics.net/2020/09/01/financial-industry-targeted-by-ransomware-hackers/

PCI Security Standards (2021). *PCI Forensic Investigator (PFI) Program*. Pcisecuritystandards.org. Retrieved April 2, 2021 from https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

Raj, D. D. S., & Pal, D. (2021). Malware patterns detection and prediction using cloud based deep learning for secured network environment. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.01.611

SANS Institute. (2021). *Information security policy templates*. Sans.org. Retrieved April 24, 2021 from https://www.sans.org/information-security-policy/?&category=application-security,general,server-security,network-security

Savin, V. D. (2021). Cyber-Security in the new era of integrated operation-informational technology systems. *Business Excellence and Management, 11*(1), 68–79. https://doi.org/10.24818/beman/2021.11.1-05

Singh, K. K. V., & Gupta, H. (2016). A new approach for the security of VPN. In Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies. 1-5.

Sony (2011, May 3). *Sony Online Entertainment Issues Security Press Release*. PlayStation.Blog. Retrieved April 2, 2021 from https://blog.playstation.com/archive/2011/05/03/sony-online-entertainment-issues-security-press-release/

Wilder, J. (2020, November 2). *PCI compliance policy requirements & template*. PCI Compliance Guide. Retrieved April 24, 2021 from https://www.pcicomplianceguide.org/understanding-and-meeting-pci-compliance-policy-requirements/

Yantz, M. (2019, November 7). *PCI Compliance: Comprehensive Guide to Protect Your Customers and Brand*. IT Support Guys. Retrieved April 10, 2021 from https://itsupportguys.com/it-blog/pci-compliance-comprehensive-guide-to-protect-your-customers-and-brand/