

[Organization]

Information Technology

Policies and Procedures

(ITPP)

[Date]

[Organization Logo]

Prepared by

| Identification of Organization that Prepared this Document | | |
| --- | --- | --- |
|  | Organization Name | The PMC Group LLC |
|  | Street Address | 14812 Sun Meadow Ct |
|  | Suite/Room/Building | Suite 101 |
|  | City, State Zip | Centreville, VA 20120 |

Prepared for

| Identification of Organization | | |
| --- | --- | --- |
|  | Organization Name |  |
| Street Address |  |
| Suite/Room/Building |  |
| City, State Zip |  |

# Template Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Page(s)** | **Description** | **Author** |
| 05/16/2017 | All | Initial Creation | Michael Chipley |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# EXECUTIVE SUMMARY

Based on Federal requirements and mandates, [Organization] ([Org. Abbr.]), is responsible for ensuring that [Organization] meets the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication (PUB) 200, Minimum Security Requirements for Federal information and information Systems and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal information Systems and Organizations. [Organization] management is fully committed to the protection of corporate and client information and has sanctioned the development of these IT Policies, associated requirements and standards to ensure the integrity, confidentiality, and availability of its information and information systems, and to ensure that it is adhering to NIST guidance to adequately implement security controls in support of federal information systems.

## Table of Contents

[Template Revision History 3](#_Toc480627634)

[EXECUTIVE SUMMARY 4](#_Toc480627635)

[Table of Contents 5](#_Toc480627636)

[Policy Level: Corporate 7](#_Toc480627637)

[Policy Terminology 7](#_Toc480627638)

[Roles and Responsibilities 8](#_Toc480627639)

[All [Organization] Employees and Contractors 8](#_Toc480627640)

[Managers and Supervisors 9](#_Toc480627641)

[Information Owners 9](#_Toc480627642)

[IT Architecture Staff 10](#_Toc480627643)

[[Organization] Application Developer Staff 10](#_Toc480627644)

[[Organization] Executive Management: CEO/President and COO/Vice President of [Organization] 11](#_Toc480627645)

[IT Security 11](#_Toc480627646)

[Incident Response Team 11](#_Toc480627647)

[Information Security Program Management (PM) 12](#_Toc480627648)

[Information Security Program Plan 12](#_Toc480627649)

[Authorizing Official (AO) 12](#_Toc480627650)

[Information Systems Security Officer (ISSO) 12](#_Toc480627651)

[Information Systems Security Manager (ISSM) 13](#_Toc480627652)

[Information Security Resources 13](#_Toc480627653)

[Plan of Action and Milestones Process 13](#_Toc480627654)

[Information System Inventory 13](#_Toc480627655)

[Information Security Measures of Performance 13](#_Toc480627656)

[Enterprise Architecture 13](#_Toc480627657)

[Critical Infrastructure Plan 13](#_Toc480627658)

[Risk Management Strategy 14](#_Toc480627659)

[Security Authorization Process 14](#_Toc480627660)

[Mission/Business Process Definition 14](#_Toc480627661)

[Insider Threat Program 14](#_Toc480627662)

[Information Security Workforce 14](#_Toc480627663)

[Testing, Training, and Monitoring 14](#_Toc480627664)

[Contacts with Security Groups and Associations 15](#_Toc480627665)

[Threat Awareness Program 15](#_Toc480627666)

[IT Policies 16](#_Toc480627667)

[Acceptable Encryption Policy 16](#_Toc480627668)

[Acceptable use Policy 19](#_Toc480627669)

[Account Management Policy 23](#_Toc480627670)

[Audit Policy 25](#_Toc480627671)

[Awareness and Training Policy 27](#_Toc480627672)

[Configuration Management Policy 29](#_Toc480627673)

[Email Policy 31](#_Toc480627674)

[Human Resources Policy 32](#_Toc480627675)

[Information Sensitivity Policy 36](#_Toc480627676)

[Password Construction Policy 43](#_Toc480627677)

[Password Protection Policy 45](#_Toc480627678)

[Penetration Testing Policy 48](#_Toc480627679)

[Remote Access Policy 65](#_Toc480627680)

[Software Installation Policy 68](#_Toc480627681)

[Vulnerability Management Policy 70](#_Toc480627682)

[Wireless Communication Policy 74](#_Toc480627683)

[Wireless Communication Standard 76](#_Toc480627684)

[Workstation Security Policy 78](#_Toc480627685)

# Policy Level: Corporate

## Policy Terminology

1. **Adverse Events:** Events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
2. **Computer security incident:** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents include:
   1. An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
   2. Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
   3. An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
   4. A user provides or exposes sensitive information to others through peer-to-peer file sharing services
3. **Event:** Any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
4. **Information:** the collection of [Organization] and or client data including but not limited to content or data captured or stored in electronic or non-electronic formats.
5. **Information Owner:** [Organization] staff member who is responsible for managing an information collection is the information owner. Typically the information owner is the head of the group on whose behalf the information is collected, oversees the project for which the information is being maintained, or is [Organization] staff member who is most closely associated with the information.
6. **Personally Identifiable Information:** (or “PII,” as used in this Policy) is information that can be used (either alone or in combination with other information) to identify, contact, or locate a unique person. Examples include, but are not limited to:
   1. name
   2. social security number
   3. address
   4. birth date
   5. telephone number
   6. account numbers
7. **Protected Health Information** (or “PHI”, as used in this Policy) is individually identifiable health information that can be linked (either alone or in combination with other information) to a particular person. Common identifiers of health information include names, social security numbers, addresses, and birth dates. Examples include (but are not limited to):
   1. The individual's past, present or future physical or mental health or condition
   2. The provision of health care to the individual
   3. The past, present, or future payment for the provision of health care to the individual.
8. **Sensitive Data (information):** is defined as information that is protected against unwarranted disclosure. Access to sensitive information should be safeguarded. Protection of sensitive information may be required for legal or ethical reasons, for issues pertaining to personal privacy, or for proprietary considerations. Sensitive Information includes all data, in its original and duplicate form, and may be in the form of:
   1. Personal Information
   2. Protected Health Information, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
   3. Student education records, as defined by the Family Educational Rights and Privacy Act (FERPA)
   4. Customer record information, as defined by the Gramm Leach Bliley Act (GLBA)
   5. Card holder data, as defined by the Payment Card Industry (PCI) information Security Standard
   6. Confidential personal data
   7. Information that is deemed to be confidential in accordance with state, local and federal Public Record Acts (Controlled Unclassified Information (CUI))
9. **Services:** Information technology consisting of systems, components, and functionality necessary for mission and business success that will require security controls to mitigate the potential risk to [Organization] through their use.

## Roles and Responsibilities

### All [Organization] Employees and Contractors

* May only access information needed to perform legitimate duties as a [Organization] employee and only when authorized by the appropriate information owner or designees.
* Are expected to ascertain and understand the sensitivity level of information to which he/she has access - through training, other resources, or by consultation with his/her supervisor or the information owner.
* May not in any way divulge, copy, release, sell, loan, alter, or destroy any information except as authorized by the information owner and within the scope of his/her professional activities.
* Must understand and comply with [Organization]’s requirements related to Personally Identifiable information (PII), Protected Health Information (PHI), and Controlled Unclassified Information (CUI).
* Must adhere to [Organization]’s requirements for protecting any computer used to conduct [Organization] business, regardless of the sensitivity level of the information held on that system.
* Must protect the confidentiality, integrity, and availability of [Organization] and client information - as appropriate for the information’s sensitivity level - wherever the information is located(e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation).
* Must handle information deemed confidential or highly confidential under this policy in accordance with [Organization]’s requirements for protecting confidential and highly confidential information.
* Must safeguard any physical key, ID card, or computer/network account that allows access to [Organization] information. This includes creating computer passwords that are compliant with the standards set forth in applicable [Organization] password policies and procedures.
* Must destroy or render unusable any confidential or highly confidential information contained in any physical document (e.g., memos, reports) or any electronic, magnetic, or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) before it is discarded in a method that is in compliance with applicable [Organization] media sanitization policies and procedures.
* Must report any activities that he/she suspects may compromise sensitive information to his/her supervisor or to [Organization] Information Systems Security Officer.
* Must report any incidents as defined in [Organization]’s Information Security Incident Reporting procedures to initiate an incident investigation.
* Must meet obligations to protect sensitive information even after [Organization] employment ends.
* Must contact [Organization] Information Systems Security Officer and the Contracts Department before complying with any court orders, subpoenas, or other compulsory requests from Federal, state, or law enforcement agencies for disclosure of confidential information.
* If performing work in an office that handles information subject to specific security regulations, must comply with additional training and documentation requirements (e.g., acknowledge annually that he/she has read, understands, and agrees to comply with the terms of this policy).

### Managers and Supervisors

In addition to complying with the requirements listed above for all employees and contractors, managers and supervisors must:

* Ensure that group or project procedures support the objectives of confidentiality, integrity, and availability as defined by the information owner and designees, and that those procedures are documented and are followed.
* Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process, or transfer the information in any form: physical or electronic.
* Ensure that each staff member understands his or her information security-related responsibilities.

### Information Owners

In addition to complying with the requirements listed above, information owners are responsible for:

* Working with [Organization]’s IT Security Officer or designee to understand the restrictions on the access and use of information as defined by federal and state laws and contractual obligations.
* Segregating the information for which he or she is responsible into logical groupings, called information collections.
* Defining the confidentiality, integrity, and availability requirements (sensitivity level) for each of his or her information collections.
* Conveying in writing the sensitivity level of each information collection for which he or she is responsible to the managers of departments that will have access to the collection.
* Working with division managers to determine what users, groups, roles, or job functions will be authorized to access the information collection and in what manner (e.g., who can view the information, who can update the information).

### IT Architecture Staff

In addition to complying with the policy requirements defined for all employees and contractors, managers and supervisors, those who manage computing and network environments that capture, store, process, and/or transmit Client or [Organization] information, are responsible for ensuring that the requirements for confidentiality, integrity, and availability, as defined by the appropriate information owner, are being satisfied within their managed information system environments. This includes:

* Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.
* Developing, implementing, operating, and maintaining a secure technology environment that includes:
  + A cohesive architectural approach
  + Product implementation and configuration standards
  + Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the information owners
  + An effective strategy for protecting information against common threats posed by computer hackers that adheres to industry-accepted “best practices” for the technology
* Ensuring that staff members understand the sensitivity levels of the data being handled and the measures used to secure it.

### [Organization] Application Developer Staff

In addition to complying with the policy requirements defined for all employees and contractors, managers and supervisors, those who develop application software to store, process, and/or transmit Client or [Organization] information, are responsible for ensuring that the requirements for confidentiality, integrity, and availability, as defined by the appropriate information owner, are being satisfied within their systems throughout the SDLC. This includes:

* Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.
* Developing, implementing, operating, and maintaining a secure technology environment that includes:
  + A cohesive architectural approach
  + Product implementation and configuration standards
  + Procedures and guidelines for administering system and application accounts and access privileges in a manner that satisfies the security requirements defined by the information owners
  + An effective strategy for protecting information against common threats posed by computer hackers that adheres to industry-accepted “best practices” for the technology
* Ensuring that staff members understand the sensitivity levels of the data being handled and the measures used to secure it.

### [Organization] Executive Management: CEO/President and COO/Vice President of [Organization]

In addition to complying with the policy requirements defined for all employees and contractors, [Organization]’s Executive Management will:

* Review and authorize information security policies
* Review, assess and authorize all configuration changes to information systems

### IT Security

In addition to complying with the policy requirements defined for IT Architecture staff, those holding roles in IT Security will be responsible for the oversight of all security functions for [Organization], to include:

* Conducting security assessments of information systems.
* Developing and maintaining security documentation for information systems.
* Perform routine audits for security impacts to systems.
* Conduct risk assessments in conjunction with the implementation of systems and as part of [Organization]’s change control process throughout the life cycle of the information system

### Incident Response Team

Members of the incident response team are required to follow the requirements associated with their respective membership in the other groups defined in section 7 but also have the responsibility of:

* Be available for anyone who discovers or suspects that an incident involving the organization has occurred
* Analyze the incident data,
* Determine the impact of the incident, and
* Act appropriately to limit the damage and restore normal services.
* Directing all communication queries to executive management to facilitate notifications to:
  + System Owner
  + Media
  + Law Enforcement
  + Vendors
  + Other Response Teams

Other notification flows will be managed through the supplemental system and or project incident reporting plans and or procedures

The incident response team is granted the authority to:

1. Confiscate or disconnect equipment and to monitor suspicious activity,
2. Report security related incidents only to executive management for evaluation and upward reporting
   1. Executive management will hold the responsibility for reporting up to [Organization] clients and to US-CERT

## Information Security Program Management (PM)

The Federal Information Security Management Act (FISMA) requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security program management (PM) controls described in this section are typically implemented at the organization level and not directed at individual organizational information systems. The program management controls have been designed to facilitate compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The controls are independent of any FIPS Publication 200 impact levels and therefore, are not directly associated with any of the security control baselines. The program management controls do, however, complement security controls and focus on the programmatic, organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

### Information Security Program Plan

[Organization] will develop and disseminate an organization-wide information security program plan to:

1. Provide an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
2. Include the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
3. Reflect coordination among [Organization] entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical); and
4. Is approved by a senior official with responsibility and accountability for the risk being incurred to [Organization] operations (including mission, functions, image, and reputation), assets, individuals, other organizations, and the Nation;

[Organization] will:

1. review [Organization]-wide information security program plan
2. Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and
3. Protects the information security program plan from unauthorized disclosure and modification.

### Authorizing Official (AO)

[Organization] will appoint an Authorizing Official (AO) with the responsibility to accept the risk and approve the organizations information systems Authority To Operate (ATO) and the information security program.

### Information Systems Security Officer (ISSO)

[Organization] will appoint a Information Systems Security Officer (ISSO) with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

### Information Systems Security Manager (ISSM)

[Organization] will appoint a Information Systems Security Manager (ISSM) with the mission and resources to coordinate, develop, implement, and maintain project specific information security programs.

### Information Security Resources

[Organization] will ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

[Organization] will employ a business case to record the resources required; and will ensure that information security resources are available for expenditure as planned.

### Plan of Action and Milestones Process

[Organization] will implement a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:

1. Are developed and maintained;
2. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
3. Are reported in accordance with OMB FISMA reporting requirements.

[Organization] will review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

### Information System Inventory

[Organization] will develop and maintain an inventory of its information systems.

### Information Security Measures of Performance

[Organization] will develop, monitor, and report on the results of information security measures of performance.

### Enterprise Architecture

[Organization] will develop an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

### Critical Infrastructure Plan

[Organization] will address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

### Risk Management Strategy

[Organization] will:

1. develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems;
2. Implements the risk management strategy consistently across the organization; and
3. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.

### Security Authorization Process

[Organization] will:

1. Manage (i.e., document, track, and report) the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
2. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
3. Fully integrate the security authorization processes into an organization-wide risk management program.

### Mission/Business Process Definition

[Organization] will:

1. Define mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
2. Determine information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained

### Insider Threat Program

[Organization] will implement an insider threat program that includes a cross-discipline insider threat incident handling team.

### Information Security Workforce

[Organization] will establish an information security workforce development and improvement program.

### Testing, Training, and Monitoring

[Organization] will:

1. Implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:
   1. Are developed and maintained; and
   2. Continue to be executed in a timely manner;
2. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

### Contacts with Security Groups and Associations

[Organization] will establish and institutionalize contact with selected groups and associations within the security community:

1. To facilitate ongoing security education and training for organizational personnel;
2. To maintain currency with recommended security practices, techniques, and technologies; and
3. To share current security-related information including threats, vulnerabilities, and incidents.

### Threat Awareness Program

[Organization] will implement a threat awareness program that includes a cross-organization information-sharing capability.

## IT Policies

The following IT Policies apply to all [Organization] information and information systems.

### Acceptable Encryption Policy

This Information Technology Acceptable Encryption Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. This policy provides guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

#### 1.0) Introduction

[Organization] Information Security Department’s intentions for publishing an Acceptable Encryption Policy are not to impose restrictions that are contrary to [Organization] established culture of openness, trust and integrity. [Organization] Information Security Manager is committed to protecting [Organization] 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 [Organization]. 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 [Organization] 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.

#### 2.0) Purpose

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 Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

#### 3.0) Scope

This policy applies to all [Organization] employees and affiliates.

#### 4.0) Policy

The Acceptable Encryption Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as [Organization] Confidential information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of [Organization] Confidential information in question.

##### 4.1) Algorithm Requirements

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

##### 4.2) Hash Function Requirements

In general, [Organization] adheres to the NIST Policy on Hash Functions.

##### 4.3) Key Agreement and Authentication

* 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.

##### 4.4) Key Generation

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

#### 5.0) Compliance

[Organization] Information Security Manager 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. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Random Number Generator (RNG) | A random number generator (RNG) is a computational or physical device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. appear random. |

#### Appendix A) Signature Algorithms

|  |  |  |
| --- | --- | --- |
| **Algorithm** | **Key Length**  **(min)** | **Additional Comment** |
| ECDSA | P-256 | Cisco recommends RFC6090 compliance to avoid patent infringement. |
| RSA | 2048 | Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required. |
| LDWM | SHA256 | A LDWM private key MUST be used only one time, and the LDWM private key MUST NOT be used for any other purpose. |

### Acceptable use Policy

This Information Technology Acceptable Use Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides a comprehensive guide for users of systems to ensure IT device usage is in line with [Organization] code of conduct and actions are in line with behaviors that are deemed acceptable.

#### 1.0) Introduction

[Organization] Information Security Department’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to [Organization] established culture of openness, trust and integrity. [Organization] Information Security Manager is committed to protecting [Organization] 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 [Organization]. 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. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every [Organization] 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.

#### 2.0) Purpose

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

#### 3.0) Scope

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

#### 4.0) Policy

##### 4.1) General Use & Ownership

1. While [Organization] network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of [Organization]. Because of the need to protect [Organization] network, management cannot guarantee the confidentiality of information stored on any network device belonging to [Organization]
2. 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.
3. [Organization] Information Security Manager recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see [Organization] Information Sensitivity Policy.
4. For security and network maintenance purposes, authorized individuals within [Organization] may monitor equipment, systems and network traffic at any time, per [Organization] Audit Policy.
5. [Organization] reserves the right to audit networks and systems on a periodic basis to ensure compliance with [Organization] Audit Policy.

##### 4.2) Security & Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less (depending on if it is a workstation or laptop), or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with [Organization] Acceptable Encryption Policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Laptops should be handled with care and treated in a sensitive manner, extreme caution should be utilized to ensure unauthorized access to the laptops does not occur.
6. Postings by employees from a [Organization] email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of [Organization], unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to [Organization] Internet/Intranet/Extranet, whether owned by the employee or [Organization], shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

##### 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 [Organization] authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing [Organization]-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.

##### 4.4) System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. 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 [Organization]
2. 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 [Organization] or the end user does not have an active license is strictly prohibited.
3. 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.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
5. 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.
6. Using a [Organization] 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.
7. Making fraudulent offers of products, items, or services originating from any [Organization] account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification to [Organization] Information Security Department’s is made.
11. 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.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. 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.
15. Providing information about, or lists of, [Organization] employees to parties outside [Organization]

##### 4.5) Email & Communications Activities

1. 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).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. 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.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within [Organization] networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by [Organization] or connected via [Organization] network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

##### 4.6) Blogging

1. Blogging by employees, whether using [Organization] 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 [Organization] IT Systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate [Organization] policy, is not detrimental to [Organization] best interests, and does not interfere with an employee's regular work duties. Blogging from [Organization] IT Systems is also subject to monitoring.
2. [Organization] Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any [Organization] confidential or proprietary information, trade secrets or any other material covered by [Organization] Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of [Organization] and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by [Organization].
4. Employees may also not attribute personal statements, opinions or beliefs to [Organization] 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 [Organization]. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, [Organization] trademarks, logos and any other [Organization] intellectual property may also not be used in connection with any blogging activity

#### 5.0) Enforcement

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

#### 6.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Blogging | Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption. |
| Spam | Unauthorized and/or unsolicited electronic mass mailings. |

### Account Management Policy

This Information Technology Account Management Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides guidelines for account management of accounts associated with [Organization].

#### 1.0) Introduction

See Purpose.

#### 2.0) Purpose

The purpose of this policy is to establish a standard for the creation, administration, use and removal of accounts that facilitate access to information and technology resources at [Organization].com account, at minimum, consists of a user ID and a password and may also include other types of information needed by the individual to perform their work.

#### 3.0) Scope

This policy is applicable to individuals that, through the use of an account, access information and technology resources at [Organization] as well as those responsible for the management of accounts or access to shared information or network. This policy covers departmental accounts as well as those managed centrally.

#### 4.0) Policy

Accounts that access electronic computing and information resources require prudent oversight. The following security standards are a part of [Organization] account management environment.

##### 4.1) Account Administration

* The owners of [Organization] data, shall make decisions regarding access to their data. Account setup and modification require the approval of the requestor's supervisor.
* The organization responsible for an information or technology resource is responsible for the activation of accounts as well as the application of appropriate security classes under the principle of “least required access” to perform their business function.
* The organization responsible for an information or technology resource is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.
* The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.
* Passwords for new accounts should NOT be emailed to remote users.
* The date when the account was issued should be recorded in an audit log

##### 4.2) Account Management

* All accounts shall be reviewed at least annually by [Organization] Information Security Manager to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. [Organization] Information Security Manager may also conduct periodic reviews for any system connected to [Organization] network.
* All guest accounts (for those who are not official members of [Organization] community) with access to [Organization] computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.
* All accounts may be disabled, revoked or deleted if account privileges are no longer commensurate with an individual’s function at [Organization] or their need-to-know due to changes in their status.
* All accounts may be disabled, revoked or deleted if it is determined the account has been compromised or misused and may only be reinstated at the direction of [Organization] Information Security Department.

##### 4.3) Individual Account Standards

* Users are responsible for all activity performed with their [Organization] ID. [Organization] IDs may not be utilized by anyone but the individuals to whom they have been issued. Users must not allow others to perform any activity with their [Organization] IDs. Similarly, users are forbidden from performing any activity with [Organization] IDs belonging to other users. Any suspected unauthorized access of a user account should be reported immediately to [Organization] Information Security Department.
* Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other mechanisms, so long as doing so does not violate any [Organization] endorsed policies. All users are responsible for both the protection of their user account password and the data stored in their user account in accordance with both [Organization] Password Protection Policy as well as [Organization] Password Construction Policy.

##### 4.3) Shared Accounts

Use of shared accounts is not allowed. Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Account | Any combination of a User ID (sometimes referred to as a username) and a password that grants an individual user access to a computer, an application, the network or any other information or technology resource. |

### Audit Policy

This Information Technology Audit Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides an overview of the audit policy in regard to [Organization] Information systems.

#### 1.0) Introduction

[Organization] Information Security Department’s intentions for publishing an Audit Policy are not to impose restrictions that are contrary to [Organization] established culture of openness, trust and integrity. [Organization] Information Security Manager is committed to protecting [Organization] 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 [Organization]. 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. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every [Organization] 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.

#### 2.0) Purpose

To provide the authority for members of [Organization] Information Security Manager to conduct a security audit on any system at any time at [Organization].

Audits may be conducted to:

* Ensure integrity, confidentiality and availability of information and resources
* Investigate possible security incidents ensure conformance to [Organization] security policies
* Monitor user or system activity where appropriate.

#### 3.0) Scope

This policy covers all computer and communication devices owned or operated by [Organization]. This policy also covers any computer and communications device that are present on [Organization] premises, but which may not be owned or operated by [Organization].

#### 4.0) Policy

When requested, and for the purpose of performing an audit, any access needed will be provided to members of [Organization] Information Security Department.

This access may include:

* User level and/or system level access to any computing or communications device
* Access to information (electronic, hard copy, etc.) that may be produced, transmitted or stored on [Organization] equipment or premises
* Access to work areas (labs, offices, cubicles, storage areas, etc.)
* Access to interactively monitor and log traffic on [Organization] networks.

#### 5.0) Enforcement

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

### Awareness and Training Policy

This Information Technology Awareness and Training Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides security and awareness principals to [Organization] such that systems within [Organization] are handled correctly.

#### 1.0) Introduction

See Purpose.

#### 2.0) Purpose

This policy establishes the Enterprise Security Awareness and Training Policy, for managing risks from a lack of company security awareness, communication, and training through the establishment of an effective security awareness and education program. The security awareness and education program helps [Organization] document, communicate, and train company personnel on security best practices and concepts.

#### 3.0) Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by [Organization]. Any information, not specifically identified as the property of other parties, that is transmitted or stored on [Organization] IT resources (including e-mail, messages and files) is the property of [Organization]. All users ([Organization] employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

#### 4.0) Policy

[Organization] has chosen to adopt the Security and Awarenessprinciples established in NIST SP 800-16 “Information Technology Security Training Requirements: A Role- and Performance-Based Model.” The following subsections outline the Security and Awarenessstandards that constitute [Organization] policy. Each [Organization] Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

* AT-1 Security Awareness and Training Policy and Procedures: All [Organization] Business Systems must develop, adopt or adhere to a formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
* AT-2 Security Awareness: All [Organization] Business Systems must provide basic security awareness training to all information asset users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and annually thereafter.
* AT-3 Security Training: All [Organization] Business Systems must provide role-based security-related training as part of initial training for new users and when required by system changes.
* AT-4 Security Training Records: All [Organization] Business Systems must:
  + Document and monitor individual information asset security training activities including basic security awareness training and specific information asset security training.
  + Retain individual training records for a year.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

### Configuration Management Policy

This Information Technology Configuration Management Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides a plan to manage risks from system changes impacting baseline configuration settings, system configuration and security.

#### 1.0) Introduction

See Purpose.

#### 2.0) Purpose

This policy establishes the Enterprise Configuration Management Policy, for managing risks from system changes impacting baseline configuration settings, system configuration and security. The configuration management program helps [Organization] document, authorize, manage and control system changes impacting Information Systems.

#### 3.0) Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by [Organization]. Any information, not specifically identified as the property of other parties, that is transmitted or stored on [Organization] IT resources (including e-mail, messages and files) is the property of [Organization]. All users ([Organization] employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

#### 4.0) Policy

[Organization] has chosen to adopt the Configuration Management principles established in NIST SP 800-53 “Configuration Management,” Control Family guidelines, as the official policy for this domain. The following subsections outline the Configuration Management standards that constitute [Organization] policy. Each [Organization] Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

* CM-1 Configuration Management Policy and Procedures: All [Organization] Business Systems must develop, adopt or adhere to a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
* CM-2 Baseline Configuration: All [Organization] Business Systems must develop, document, and maintain a current baseline configuration of their Information Systems. The baseline configuration must be reviewed and updated based on environment changes.
* CM-3 Configuration Change Control: All [Organization] Business Systems must perform change control for key Information Systems. This includes:
  + Determining the type of changes to the information asset that are configuration controlled.
  + Approving configuration-controlled changes to the system with explicit consideration for security impact analysis.
  + Documenting approved configuration-controlled changes to the system.
  + Retaining and reviewing records of configuration-controlled changes to the system.
  + Auditing activities associated with configuration-controlled changes to the system.
  + Coordinating and providing oversight for configuration change control activities through Change Control Board (CCB) that convenes weekly.
* CM-4 Security Impact Analysis: All [Organization] Business Systems must analyze changes to the Information Systems to determine potential security impacts prior to change implementation.
* CM-5 Access Restrictions for Change: All [Organization] Business Systems must define, document, approve, and enforce physical and logical access restrictions with changes to the information asset.
* CM-6 Configuration Settings: All [Organization] Business Systems must establish, document, implement and monitor mandatory configuration settings for information technology products employed within the information asset using a security configuration checklist that reflects the most restrictive mode consistent with operational requirements. In addition, any exceptions to the mandatory configuration settings within the information asset must be identified, documented, and approved prior to ongoing use.
* CM-7 Least Functionality: All [Organization] Business Systems must configure the information asset to provide only essential capabilities and specifically prohibit or restrict the use of the following functions, ports, protocols, and/or services.
* CM-8 Information System Component Inventory: All [Organization] Business Systems must develop, document, and maintain an inventory of the information asset components that exist within their area. Inventory detail must be maintained at a sufficient level for purposes of tracking and reporting.
* CM-9 Configuration Management Plan: All [Organization] Business Systems must develop, document, and implement a configuration management plan for the information asset that:
  + Addresses roles, responsibilities, and configuration management processes and procedures.
  + Defines the configuration items for the information asset and when in the system development life cycle the configuration items are placed under configuration management.
  + Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

### Email Policy

This Information Technology Email Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. This policy outlines the minimum requirements for use of email within [Organization] Network.

#### 1.0) Introduction

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it’s important for users to understand the appropriate use of electronic communications.

#### 2.0) Purpose

The purpose of this email policy is to ensure the proper use of [Organization] email system and make users aware of what [Organization] deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within [Organization] Network.

#### 3.0) Scope

This policy covers appropriate use of any email sent from a [Organization] email address and applies to all employees, vendors, and agents operating on behalf of [Organization].

#### 4.0) Policy

* All use of email must be consistent with [Organization] policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
* [Organization] email account should be used primarily for [Organization] business-related purposes; personal communication is permitted on a limited basis, but non-[Organization] related commercial uses are prohibited.
* All [Organization] data contained within an email message or an attachment must be secured according to the Data Protection Standard.
* Email should be retained only if it qualifies as a [Organization] business record. Email is a [Organization] business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
* Email that is identified as a [Organization] business record shall be retained according to [Organization] Record Retention Schedule.
* [Organization] email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any [Organization] employee should report the matter to their supervisor immediately.
* Users are prohibited from automatically forwarding [Organization] email to a third party email system. Individual messages which are forwarded by the user must not contain [Organization] confidential or above information.
* Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct [Organization] business, to create or memorialize any binding transactions, or to store or retain email on behalf of [Organization] Such communications and transactions should be conducted through proper channels using [Organization]-approved documentation.
* Using a reasonable amount of [Organization] resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a [Organization] email account is prohibited.
* [Organization] employees shall have no expectation of privacy in anything they store, send or receive on the company’s email system.
* [Organization] may monitor messages without prior notice. [Organization] is not obliged to monitor email messages.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

### Human Resources Policy

This Information Technology Human Resources Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. This policy outlines the new hire and termination processes of IT assets connecting to [Organization] network.

#### 1.0) Introduction

Anyone who has access to [Organization] information and information systems must be an authorized user.

#### 2.0) Purpose

The purpose of this Human Resource policy is to ensure the all new users any terminated users accounts and IT assets are properly configured and managed throughout the life-cycle of the network access.

#### 3.0) Scope

This policy applies to all employees, vendors, and agents operating on behalf of [Organization].

#### 4.0) Policy

##### 4.1) New Hire Process

* 1. This is unique to each organization

##### 4.2) Termination Process

1. This is unique to each organization

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

### Information Sensitivity Policy

This Information Technology Information Sensitivity Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides an overview of the information security policy in regard to [Organization]

#### 1.0) Introduction

[Organization] Information Security Department’s intentions for publishing an Information Sensitivity Policy are not to impose restrictions that are contrary to [Organization] established culture of openness, trust and integrity. [Organization] Information Security Manager is committed to protecting [Organization] 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 [Organization]. 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. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every [Organization] 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.

#### 2.0) Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of [Organization] without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect [Organization] Confidential information (e.g., [Organization] Confidential information should not be left unattended in conference rooms).

*Note: The impact of these guidelines on daily activity should be minimal.*

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to [Organization] Information Security Department.

#### 3.0) Scope

All [Organization] Information is categorized into two main classifications:

* [Organization] Public
* [Organization] Confidential

[Organization] Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to [Organization]

[Organization] Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in [Organization] Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of [Organization] Confidential information is "[Organization] Third Party Confidential" information. This is confidential information belonging or pertaining to another organization which has been entrusted to [Organization] by that organization under nondisclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, supplier information and federal information/data. Information in this category ranges from extremely sensitive (controlled unclassified information) to information about the fact that we've connected a supplier / vendor / federal organization into [Organization] network to support our operations.

[Organization] personnel are encouraged to use common sense judgment in securing [Organization] Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should contact their manager for clarification.

Technical information will be labeled “Controlled Unclassified Information – Technical Information”.

#### 4.0) Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as [Organization] Confidential information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of [Organization] Confidential information in question.

##### 4.1) Minimal Sensitivity

General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

*Note: Any of these markings may be used with the additional annotation of "3rd Party Confidential".*

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "[Organization] Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "[Organization] Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, [Organization] Information is presumed to be "[Organization] Confidential" unless expressly determined to be [Organization] Public information by a [Organization] employee with authority to do so.

* **Access**: [Organization] employees, contractors, people with a business need to know.
* **Distribution within [Organization]**: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
* **Distribution outside of [Organization] internal mail**: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
* **Electronic distribution**: No restrictions except that it be sent to only approved recipients.
* **Storage**: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
* **Disposal/Destruction**: Deposit outdated paper information in specially marked disposal bins on [Organization] premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
* **Penalty for deliberate or inadvertent disclosure**: Up to and including termination, possible Civil and/or criminal prosecution to the full extent of the law.

##### 4.2) More Sensitive

Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

*Note: Any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "[Organization] Confidential" or "[Organization] Proprietary", wish to label the information "[Organization] Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.*

* **Access**: [Organization] employees and non-employees with signed non-disclosure agreements who have a business need to know.
* **Distribution within [Organization]**: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
* **Distribution outside of [Organization] internal mail**: Sent via U.S. mail or approved private carriers.
* **Electronic distribution**: No restrictions to approved recipients within [Organization], but should be encrypted or sent via a private link to approved recipients outside of [Organization] premises.
* **Storage**: Individual access controls are highly recommended for electronic information.
* **Disposal/Destruction**: In specially marked disposal bins on [Organization] premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
* **Penalty for deliberate or inadvertent disclosure**: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Technical information will be labeled “Controlled Unclassified Information – Technical Information”.

##### 4.3) Most Sensitive

Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

*Note: Any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that [Organization] Confidential information is very sensitive, you may should label the information "[Organization] Internal: Registered and Restricted", "[Organization] Eyes Only", "[Organization] Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of [Organization] Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.*

* **Access**: Only those individuals ([Organization] employees and nonemployees) designated with approved access and signed non-disclosure agreements.
* **Distribution within [Organization]**: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
* **Distribution outside of [Organization] internal mail**: Delivered direct; signature required; approved private carriers.
* **Electronic distribution**: No restrictions to approved recipients within [Organization], but it is highly recommended that all information be strongly encrypted.
* **Storage**: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
* **Disposal/Destruction**: Strongly Encouraged: In specially marked disposal bins on [Organization] premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
* **Penalty for deliberate or inadvertent disclosure**: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Technical information will be labeled “Controlled Unclassified Information – Technical Information”.

#### 5.0) Enforcement

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

#### 6.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Appropriate measures | To minimize risk to [Organization] from an outside business connection. [Organization] computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access [Organization] corporate information, the amount of information at risk is minimized. |
| Configuration of [Organization] to other business connections | Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary. |
| Delivered Direct; Signature Required | Do not leave in interoffice mail slot, call the mail room for special pick-up of mail. |
| Approved Electronic File Transmission Methods | Includes supported FTP clients and Web browsers. |
| Envelopes Stamped Confidential | You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential. |
| Approved Electronic Mail | Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization. |
| Approved Encrypted email and files | Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within [Organization] is done via a license. Please contact the appropriate support organization if you require a license. |
| Company Information System Resources | Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above. |
| Expunge | To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. |
| Individual Access Controls | Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command. On Mac’s and PC's, this includes using passwords on screensavers. |
| Insecure Internet Links | Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of [Organization] |
| Encryption | Secure [Organization] Sensitive information in accordance with [Organization] Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance. |
| One Time Password Authentication | One Time Password Authentication on Internet connections is accomplished by using a one-time password token to connect to [Organization] internal network over the Internet. |
| Physical Security | Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet. |
| Private Link | A Private Link is an electronic communications path that [Organization] has control over it's entire distance. For example, all [Organization] networks are connected via a private link. |

### Password Construction Policy

This Information Technology Password Construction Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides an easy to understand construction ruleset for creation of passwords for use on the various [Organization] Information systems.

#### 1.0) 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 [Organization] network. This guideline provides best practices for creating secure passwords.

#### 2.0) Purpose

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

#### 3.0) Scope

This guideline applies to employees, contractors, consultants, temporary and other workers at [Organization], 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, email accounts, screen saver protection, voicemail, and local router logins.

#### 4.0) Policy

All passwords should meet or exceed the following guidelines

Medium to Strong passwords have the following characteristics:

* Contain at least 8 or more alphanumeric/special characters.
* Contain both upper and lower case letters.
* Contain at least one number (for example, 0-9).
* Contain at least one special character (for example,!$%^&\*()\_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

* Contain less than eight characters.
* Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
* Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
* Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
* Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
* Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
* Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

Passwords should not be recycled and when a new password is required, old passwords should no longer be used or ‘recycled’ such that the new password is the same password as previously used by the user at least in the last 24 passwords.

*Note: Do not use either of these examples as passwords*

##### 4.1) Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was\*&!$ThisMorning!).

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

### Password Protection Policy

This Information Technology Password Protection Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The policy provides a comprehensive guide to account passwords for [Organization] employees and devices to ensure secure password usage on [Organization]’s IT Systems.

#### 1.0) Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of [Organization] resources. All users, including contractors and vendors with access to [Organization] IT systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

#### 2.0) Purpose

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

#### 3.0) Scope

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

#### 4.0) Policy

All passwords should meet or exceed the following guidelines

##### 4.1) Password Creation

* All user-level and system-level passwords must conform to the Password Construction Guidelines.
* Users must not use the same password for [Organization] accounts as for other non-[Organization] access (for example, personal ISP account, option trading, benefits, and so on).
* Where possible, users must not use the same password for various [Organization] access needs.
* User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
* Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to logon interactively. SNMP community strings must meet password construction guidelines.

##### 4.2) Password Change

* All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
* All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
* Password cracking or guessing may be performed on a periodic or random basis by [Organization] Information Security Manager or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

##### 4.3) Password Protection

* Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential [Organization] Information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
* Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
* Passwords must not be revealed over the phone to anyone.
* Do not reveal a password on questionnaires or security forms.
* Do not hint at the format of a password (for example, "my family name").
* Do not share [Organization] passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
* Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
* Do not use the "Remember Password" feature of applications (for example, web browsers).
* Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

##### 4.4) Application Development

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

* Applications must support authentication of individual users, not groups.
* Applications must not store passwords in clear text or in any Applications must not transmit passwords in clear text over the network.
* Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

##### 4.5) Use of Passwords and Passphrases

The proper construction of passwords and passphrases is outlined in more detail in [Organization] Password Construction Policy, specifically in section 4.1. Assurance that strong passphrases are utilized without succumbing to the pitfalls of reduced security in favor of an easier to remember password (for example) should be avoided to maintain a high level of security in relation to [Organization] computing devices as well as use of default passwords.

Laptops that are assigned to the field teams are hardened such that brute-force attack possibilities on these systems are minimized. The laptops lock out users after three consecutive invalid attempts to gain entry to the system are detected. Brute-force attack measures as a result would be severely hampered and the combination of the lock out measures as well as the generation of passwords that would not be found in general word lists assists in the creation of a secure system in regard to password security.

The laptops that are assigned to the field have settings enabled such that passwords have no more than 42 days of lifespan before the user is forced to change their password to continue to use the system. The maximum password age assists in ensuring that if a secondary party has access to the credentials of an authorized user, their access is limited to the duration of the maximum age of the password.

A database for each user and their associated past passwords is used for comparison when creating a new password. Users are not able to choose passwords that they have previously used in the last 24 attempts. To ensure that users do not cycle their history by creating multiple new passwords in a day, in an attempt to clear the database history so they can reuse a previous password, there is also a minimum password age of one day assigned to the laptops. This setting ensures that users cannot attempt to circumvent the system to reuse old passwords.

In accordance with [Organization] Acceptable Use Policy, the workstation screensaver will enable in a short amount of time of inactivity, ~10 minutes, to ensure that if a user walks away from their desk that unauthorized access to their workstation does not occur. Tablets screensaver will enable after 30 minutes of inactivity.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| SNMP | Simple Network Management Protocol |
| ISP | Internet Service Provider |
| NT | Windows NT (Windows New Technology) |

### Penetration Testing Policy

This Information Technology Penetration Testing Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides guidelines for penetration testing in accordance with NIST 800-53A & NIST 800-115.

#### 1.0) Introduction

See Purpose.

#### 2.0) Purpose

The purpose of this penetration testing policy is to ensure that the systems that are put in place have adequate security controls and associated personnel have understanding of possibilities for exploit.

#### 3.0) Scope

The purpose of this document is to provide guidelines for [Organization] on planning and conducting technical information security testing and assessments, analyzing findings, and developing mitigation strategies. It provides practical recommendations for designing, implementing, and maintaining technical information relating to security testing and assessment processes and procedures, which can be used for several purposes—such as finding vulnerabilities in a system or network and verifying compliance with a policy or other requirements.

#### 4.0) Policy

Penetration testing on Amazon Web Services requires submission of information about the instances you wish to test, identify the expected start and end dates/times of your test, and requires you to read and agree to Terms and Conditions specific to penetration testing and to the use of appropriate tools for testing. Note that the end date may not be more than 3 months from the start date.

The information shared with AWS as part of this process is kept confidential within AWS. The following guidelines that will be utilized will be shared with AWS such that approval can be provided to begin penetration testing before any penetration testing or vulnerability assessment begins.

##### 4.1) Penetration Testing Phases

Penetration testing is most commonly completed through four stages: Planning, Discovery, Attack & Reporting.

|  |
| --- |
|  |
| Figure 4-1 Four-Stage Penetration Testing Methodology |

In the planning phase, rules are identified, management approval is finalized and documented, and testing goals are set. The planning phase sets the groundwork for a successful penetration test. No actual testing occurs in this phase. During the planning phase of the penetration test, a rules of engagement document should be completed, detailing the start and end dates of the penetration test as well as associated targets and contact information for personnel involved with the project. As [Organization] Mobile app is hosted on AWS, AWS needs to be notified and associated documentation should be provided including much of the information contained within the rules of engagement document to provide AWS with information needed to conduct such a test on their systems.

The discovery phase of penetration testing includes two parts. The first part is the start of actual testing, and covers information gathering and scanning. Network port and service identification, described in Section 4.08, as well as social engineering, described in section 4.12, are conducted to identify potential targets. The second part of the discovery phase is vulnerability analysis, which involves comparing the services, applications, and operating systems of scanned hosts against vulnerability databases (a process that is automatic for vulnerability scanners) and the testers’ own knowledge of vulnerabilities. Human testers can use their own databases—or public databases such as the National Vulnerability Database (NVD) to identify vulnerabilities manually.

Executing an attack is at the heart of any penetration test and the third phase. If an attack is successful, the vulnerability is verified and safeguards are identified to mitigate the associated security exposure. The attack may result in the testers learning more about the targeted network and its potential vulnerabilities, or induce a change in the state of the targeted network’s security. Some exploits enable testers to escalate their privileges on the system or network to gain access to additional resources.

|  |
| --- |
|  |
| Figure 4-2 Attack Phase Steps |

Testing and analysis on multiple systems should be conducted during a penetration test to determine the level of access an adversary could gain. Enough data has been gathered in the discovery phase to make an informed attempt to guess the target during the gaining access phase of the attack. If only user-level access was obtained in the gaining access step, the assessor will seek to gain complete control of the system (administrator-level access) in the escalating privileges phase of the attack. The information gathering process begins again to identify mechanisms to gain access to additional systems in the system browsing phase which could constitute looping back to the discovery phase of the test if additional information is found. The last step of the attack phase utilizes additional tools to gain even more information or access to the system.

##### 4.2) Penetration Testing Layout

Penetration test scenarios should focus on locating and targeting exploitable defects in the design and implementation of the application, system, or network. Tests should reproduce both the most likely and most damaging attack patterns—including worst-case scenarios such as malicious actions by administrators. Since a penetration test scenario can be designed to simulate an inside attack, an outside attack, or both, external and internal security testing methods are considered. If both internal and external testing is to be performed, the external testing usually occurs first.

Since the testers’ traffic usually goes through a firewall, the amount of information obtained from scanning is far less than if the test were undertaken from an insider perspective. After identifying hosts on the network that can be reached from outside, testers attempt to compromise one of the hosts. If successful, this access may then be used to compromise other hosts that are not generally accessible from outside the network. Penetration testing is an iterative process that leverages minimal access to gain greater access.

Insider scenarios simulate the actions of a malicious insider. An internal penetration test is similar to an external test, except that the testers are on the internal network (i.e., behind the firewall) and have been granted some level of access to the network or specific network systems. Using this access, the penetration testers try to gain a greater level of access to the network and its systems through privilege escalation. Testers are provided with network information that someone with their level of access would normally have—generally as a standard employee, although depending on the goals of the test it could instead be information that a system or network administrator might possess.

##### 4.3) External Reconnaissance

External testing begins with reconnaissance techniques that search public registration data, Domain Name System (DNS) server information, newsgroup postings, and other publicly available information to collect information (e.g., system names, Internet Protocol [IP] addresses, operating systems, technical points of contact) that may help the assessor to identify vulnerabilities. Next, enumeration begins by using network discovery and scanning techniques to determine external hosts and listening services. Since perimeter defenses such as firewalls, routers, and access control lists often limit the types of traffic allowed into the internal network, assessors will use techniques that evade these defenses—just as external attackers would. External security testing also concentrates on discovering access method vulnerabilities, such as portals to internal servers.

##### 4.4) Internal Reconnaissance

For internal security testing, assessors work from the internal network and assume the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This kind of testing can reveal vulnerabilities that could be exploited, and demonstrates the potential damage this type of attacker could cause. Internal security testing also focuses on system-level security and configuration—including application and service configuration, authentication, access control, and system hardening.

An assessor could utilize their current privileges to examine the currently running processes and services on the system to examine to see if there are any unusual or unexpected processes that are running. Focus can be directed to any processes that are found with high privileges such as *SYSTEM* or *Administrator* (or other users that are in the Administrator group).

An assessor should examine the Administrators group or groups with heightened privileges through use of the Local Users and Groups control panel (*lusrmgr.msc*) to identify members of the group that should not be there. The examination could be done through a command prompt interface as well instead of using the GUI through the *net user* and *net localgroup* commands.

Simple tools such as *Windows Task Manager* or Windows’ service manager (accessible through *services.msc* or through command prompt using the *sc query* command) can be utilized to find a list of services that are unknown or known to be malicious on the machine as well as provide a list of services that are associated with each process.

##### 4.5) Log Review

Log review determines if security controls are logging the proper information, and if [Organization] is adhering to its log management policies. As a source of historical information, audit logs can be used to help validate that the system is operating in accordance with established policies. For example, if the logging policy states that all authentication attempts to critical servers must be logged, the log review will determine if this information is being collected and shows the appropriate level of detail. Log review may also reveal problems such as misconfigured services and security controls, unauthorized accesses, and attempted intrusions.

Reviewing logs can present administrators with information that could be utilized to become aware of a possible incident. SANS Institute outlines some generic log entries which could be viewed as highly unusual and may constitute further review. Log events can be found by running the Windows event viewer from an administrative account using *eventvwr.msc* or utilizing an elevated command prompt and running the *eventquery.vbs | more* command. Some examples of suspicious log entries include (but are not limited to):

* “Event log service was stopped.”
* “Windows File Protection is not active on this system.”
* “The protected System file [*particular file name*] was not restored to its original, valid version because…”
* “The MS Telnet Service has started successfully.”
* A high volume of failed logon attempts or accounts that are locked.

The process of reviewing logs can be tedious at times and require knowledge of the system being analyzed. It should be common practice to take time to review logs, even during normal operating conditions, to ensure that there is no erroneous activities happening without the knowledge of the administrator or administrative team. System administrators are at the front lines of maintaining a level of security within the system. Following best practices and maintaining a vigilant eye on generated logs ensures that system administrators have the best chance to find indications of a system compromise before it develops further.

##### 4.6) Ruleset Review

A ruleset is a collection of rules or signatures that network traffic or system activity is compared against to determine what action to take—for example, forwarding or rejecting a packet, creating an alert, or allowing a system event. Review of these rulesets is done to ensure comprehensiveness and identify gaps and weaknesses on security devices and throughout layered defenses such as network vulnerabilities, policy violations, and unintended or vulnerable communication paths. A review can also uncover inefficiencies that negatively impact a rule set's performance.

##### 4.7) Configuration Review

Automated tools are often executed directly on the device or application being assessed, but can also be executed on a system with network access to the device or application being assessed. While automated system configuration reviews are faster than manual methods, there may still be settings that must be checked manually. Both manual and automated methods require root or administrator privileges to view selected security settings.

Registry keys can be examined to identify malicious programs being referenced that are unknown to system administrators that serve no business function. An example of some registry keys that can be quickly looked through to identify possible malicious activity include (but are not limited to):

* HKLM\Software\Microsoft\Windows\CurrentVersion\Run
* HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
* HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

Generally, it is preferable to use automated checks instead of manual checks whenever feasible. Automated checks can be done very quickly and provide consistent, repeatable results. Having a person manually checking hundreds or thousands of settings is tedious and error-prone.

##### 4.8) Network and Service Identification Review

Network port and service identification involves using a port scanner to identify network ports and services operating on active hosts—such as FTP and HTTP—and the application that is running each identified service, such as Microsoft Internet Information Server (IIS) or Apache for the HTTP service.

[Organization] should conduct network port and service identification to identify hosts if this has not already been done by other means (e.g., network discovery), and flag potentially vulnerable services. This information can be used to determine targets for penetration testing.

It is recommended that if both external and internal scanning are to be used and the assessors are intentionally performing the testing “blind,” that external scanning be performed first. Done in this order, logs can be reviewed and compared before and during internal testing. When performing external scanning, assessors may use any existing stealth techniques to get packets through firewalls while evading detection by IDS and IPS. Tools that use fragmentation, duplication, overlap, out-of-order, and timing techniques to alter packets so that they blend into and appear more like normal traffic are recommended. Internal testing tends to use less aggressive scanning methods because these scans are blocked less often than external scans. Using more aggressive scans internally significantly increases the chances of disrupting operations without necessarily improving scan results. Being able to scan a network with customized packets also works well for internal testing, because checking for specific vulnerabilities requires highly customized packets. Tools with packet-builder ability are helpful with this process. Once built, packets can be sent through a second scanning program that will collect the results. Because customized packets can trigger a denial of service (DoS) attack, this type of test should be conducted during periods of low network traffic—such as overnight or on the weekend. As a result of the use of AWS as the provider for [Organization] Mobile, the testing periods should be within the constraint of approval from Amazon.

##### 4.9) Vulnerability Scanning

A vulnerability scanner is a relatively fast and easy way to quantify [Organization] exposure to surface vulnerabilities. A surface vulnerability is a weakness that exists in isolation, independent from other vulnerabilities. The system’s behaviors and outputs in response to attack patterns submitted by the scanner are compared against those that characterize the signatures of known vulnerabilities, and the tool reports any matches that are found. Besides signature-based scanning, some vulnerability scanners attempt to simulate the reconnaissance attack patterns used to probe for exposed, exploitable vulnerabilities, and report the vulnerabilities found when these techniques are successful.

Vulnerability scanning is a somewhat labor-intensive activity that requires a high degree of human involvement to interpret results. It may also disrupt network operations by taking up bandwidth and slowing response times. Nevertheless, vulnerability scanning is extremely important in ensuring that vulnerabilities are mitigated before they are discovered and exploited by adversaries.

As with all pattern-matching and signature-based tools, application vulnerability scanners typically have high false positive rates. Assessors should configure and calibrate their scanners to minimize both false positives and false negatives to the greatest possible extent, and meaningfully interpret results to identify the real vulnerabilities. Scanners also suffer from the high false negative rates that characterize other signature-based tools—but vulnerabilities that go undetected by automated scanners can potentially be caught using multiple vulnerability scanners or additional forms of testing. A common practice is to use multiple scanners—this provides assessors with a way to compare results.

##### 4.10) Bluetooth Scanning

Passive scanning for Bluetooth-enabled wireless devices should be conducted to evaluate potential presence and activity. Because Bluetooth has a very short range (on average 9 meters [30 feet], with some devices having ranges of as little as 1 meter [3 feet]), scanning for devices can be difficult and time-consuming. Assessors should take range limitations into consideration when scoping this type of scanning.

[Organization] will want to confirm compliance with their Bluetooth security requirements, passive scanning for Bluetooth-enabled wireless devices should be conducted to evaluate potential presence and activity. Because Bluetooth has a very short range (on average 9 meters [30 feet], with some devices having ranges of as little as 1 meter [3 feet]), scanning for devices can be difficult and time-consuming. Assessors should take range limitations into consideration when scoping this type of scanning.

##### 4.11) Application Password Cracking

When a user enters a password, a hash of the entered password is generated and compared with a stored hash of the user’s actual password. If the hashes match, the user is authenticated. Password cracking is the process of recovering passwords from password hashes stored in a computer system or transmitted over networks. When a user enters a password, a hash of the entered password is generated and compared with a stored hash of the user’s actual password. If the hashes match, the user is authenticated. Password cracking is the process of recovering passwords from password hashes stored in a computer system or transmitted over networks. It is usually performed during assessments to identify accounts with weak passwords. Password cracking is performed on hashes that are either intercepted by a network sniffer while being transmitted across a network, or retrieved from the target system. There are multiple forms of password cracking, some of which are explained below.

A dictionary attack is a form of password cracking which uses all words in a dictionary or text file. There are numerous dictionaries available on the Internet that encompass major and minor languages, names, popular television shows, etc. Another cracking method is known as a hybrid attack, which builds on the dictionary method by adding numeric and symbolic characters to dictionary words. Depending on the password cracker being used, this type of attack can try a number of variations, such as using common substitutions of characters and numbers for letters (e.g., p@ssword and h4ckme). Some will also try adding characters and numbers to the beginning and end of dictionary words (e.g., password99, password$%).

A brute force attack generates all possible passwords up to a certain length and their associated hashes. Since there are so many possibilities, it can take months to crack a password. Although brute force can take a long time, it usually takes far less time than most password policies specify for password changing. Consequently, passwords found during brute force attacks are still too weak. Theoretically, all passwords can be cracked by a brute force attack, given enough time and processing power, although it could take many years and require serious computing power. Assessors and attackers often have multiple machines over which they can spread the task of cracking passwords, which greatly shortens the time involved.

Rainbow tables can also be utilized for password cracking. Rainbow tables are lookup tables with pre-computed password hashes. For example, a rainbow table can be created that contains every possible password for a given character set up to a certain character length. Assessors may then search the table for the password hashes that they are trying to crack. Rainbow tables require large amounts of storage space and can take a long time to generate, but their primary shortcoming is that they may be ineffective against password hashing that utilizes salting. Salting is the inclusion of a random piece of information in the password hashing process that decreases the likelihood of identical passwords returning the same hash. Rainbow tables will not produce correct results without taking salting into account, but this dramatically increases the amount of storage space that is required for the process. Most operating systems use salted password hashing mechanisms to reduce the effectiveness of rainbow tables.

##### 4.12) Social Engineering

Social engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. It is used to test the human element and user awareness of security, and can reveal weaknesses in user behavior—such as failing to follow standard procedures. Social engineering can be performed through many means, including analog (e.g., conversations conducted in person or over the telephone) and digital (e.g., e-mail, instant messaging). One form of digital social engineering is known as phishing, where attackers attempt to steal information such as credit card numbers, Social Security numbers, user IDs, and passwords. Phishing uses authentic-looking emails to request information or direct users to a bogus website to collect information. Other examples of digital social engineering include crafting fraudulent e-mails and sending attachments that could mimic worm activity. In accordance with [Organization] Email Policy, Acceptable Use Policy, Information Sensitivity Policy and Password Protection Policy, the possibilities of social engineering should be minimized. Testing the effectiveness of these policies in a real-world scenario might expose weaknesses in the policies or in the adherence to these policies that could allow an attacker access to systems within [Organization].

|  |
| --- |
|  |
| Figure 4-3 Social Engineering |

Social engineering may be used to target specific high-value individuals or groups within [Organization], such as executives, or may have a broad target set. Specific targets may be identified when [Organization] knows of an existing threat or feels that the loss of information from a person or specific group of persons could have a significant impact. For example, phishing attacks can be targeted based on publicly available information about specific individuals (e.g., titles, areas of interest). Individual targeting can lead to embarrassment for those individuals if testers successfully elicit information or gain access. It is important that the results of social engineering testing are used to improve the security of the organization and not to single out individuals. Testers should produce a detailed final report that identifies both successful and unsuccessful tactics used. This level of detail will help [Organization] to tailor their security awareness training programs.

##### 4.13) Lessons Learned

Final analysis, such as the development of overall conclusions, usually takes place after all testing activities have been completed and involves the development of mitigation recommendations. While identifying and categorizing vulnerabilities is important, a security test is much more valuable if it also results in a mitigation strategy being developed and implemented. Mitigation recommendations, including the outcome of the root cause analysis, should be developed for each finding. There may be both technical recommendations (e.g., applying a particular patch) and nontechnical recommendations that address [Organization] processes (e.g., updating the patch management process). Examples of mitigation actions include policy, process, and procedure modifications; security architecture changes; deployment of new security technologies; and deployment of OS and application patches.

##### 4.14) Penetration Test Result Reporting

Upon completion of analysis, a report should be generated that identifies system, network, and organizational vulnerabilities and their recommended mitigation actions.

Security testing results should be documented and made available to the appropriate staff, which may include the CIO, CISO, and ISSO as well as appropriate program managers or system owners. Because a report may have multiple audiences, multiple report formats may be required to ensure that all are appropriately addressed. Internal reports should include test methodology, test results, analysis, and POA&M.38 A POA&M will ensure that individual vulnerabilities are addressed with specific, measurable, attainable, realistic, and tangible actions.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Active Security Testing | Security testing that involves direct interaction with a target such as sending packets to a target |
| Banner Grabbing | The process of capturing banner information, such as application type and version that is transmitted by a remote port when a connection is initiated. |
| Covert Testing | Testing performed using covert methods and without the knowledge of the organization’s IT staff, but with full knowledge and permission of upper management. |
| External Security Testing | Security testing conducted from outside the organization’s security perimeter |
| False Positive | An alert that incorrectly indicates that a vulnerability is present |
| File Integrity Checking | Software that generates, stores and compares message digests for files to detect changes made to the files |
| Information Security Testing | The process of validating the effective implementation of security controls for information systems and networks, based on the organization’s security requirements. |
| Internal Security Testing | Security testing conducted from inside the organization’s security perimeter. |
| Network Discovery | The process of discovering active and responding hosts on a network, identifying weakness and learning how the network operates. |
| Network Sniffing | A passive technique that monitors network communication, decodes protocols and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique. |
| Operating System Fingerprinting | Analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target. |
| Overt Testing | Security testing performed with the knowledge and consent of the organization’s IT staff. |
| Passive Security Testing | Security testing that does not involve any direct interaction with the targets, such as sending packets to a target. |
| Password Cracking | The process of recovering secret passwords stored in a computer system or transmitted over a network. |
| Penetration Testing | Security testing in which evaluators mimic real world attacks in an attempt to identify ways to circumvent the security features of an application, system or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. |
| Phishing | A digital form of social engineering that uses authentic-looking, but bogus, emails to request information from users or direct them to a fake website that requests information from those users. |
| Plan of Actions and Milestones | A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones for meeting the tasks and scheduled milestone completion dates. |
| Port Scanner | A program that can remotely determine which ports on a system are open (e.g., whether system allow connections through those ports). |
| Review Techniques | Passive information security testing techniques, generally conducted manually, that are used to evaluate systems, applications, networks, policies and procedures to discover vulnerabilities. They include documentation, log, ruleset and system configuration review; network sniffing; and file integrity checking |
| Rogue Device | An unauthorized node on a network |
| Rules of Engagement | Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test and gives the test team authority to conduct defined activities without the need for additional permissions |
| Ruleset | A collection of rules or signatures that network traffic or system activity is compared against to determine an action to take such as forwarding or rejecting a packet, creating an alert or allowing a system event. |
| Social Engineering | The process of attempting to trick someone into revealing information |
| Target Identification and Analysis Techniques | Information security testing techniques, mostly active and generally conducted using automated tools that are used to identify systems, ports, services and potential vulnerabilities. Target identification and analysis techniques include network discovery, network port and service identification, vulnerability scanning, wireless scanning and application security testing. |
| Version Scanning | The process of identifying the service application and application version currently in use |
| Vulnerability | Weakness in an information system, or in a system security procedures, internal controls or implementation that could be exploited or triggered by some threat source. |
| Vulnerability Scanning | A technique used to identify hosts or host attributes and associated vulnerabilities. |

Penetration Testing Rules of Engagement Worksheet

(<http://pen-testing.sans.org/retrieve/rules-of-engagement-worksheet.rtf>):

**Penetration Testing Team Contact Information:**

Primary Contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mobile Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Secondary Contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mobile Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Target Organization Contact Information:**

Primary Contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mobile Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Secondary Contact: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mobile Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pager: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

"Daily Debriefing" Frequency: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

"Daily Debriefing" Time/Location: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Start Date of Penetration Test: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

End Date of Penetration Test: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Testing Occurs at Following Times: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will test be announced to target personnel: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will target organization shun IP addresses of attack systems: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Does target organization's network have automatic shunning capabilities that might disrupt access in unforeseen ways (i.e. create a denial­of­service condition), and if so, what steps will be taken to

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Would the shunning of attack systems conclude the test: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If not, what steps will be taken to continue if systems get shunned and what approval (if any) will

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IP addresses of penetration testing team's attack systems:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is this a "black box" test: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the policy regarding viewing data (including potentially sensitive/confidential data) on

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will target personnel observe the testing team: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Primary Contact representing Target Organization

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Head of Penetration Testing Team

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If necessary, signatures of individual testers:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Penetration Testing Scope Worksheet

(<http://pen-testing.sans.org/retrieve/scope-worksheet.rtf>)

What are the target organization's biggest security concerns?

(Examples include disclosure of sensitive information, interruption of production processing, embarrassment due to website defacement, etc.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What specific hosts, network address ranges, or applications should be tested?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What specific hosts, network address ranges, or applications should explicitly NOT be tested?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

List any third parties that own systems or networks that are in scope as well as which systems they own (written permission must have been obtained in advance by the target organization)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will the test be performed against a live production environment or a test environment?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will the penetration test include the following testing techniques?

Ping sweep of network ranges: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Port scan of target hosts: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Vulnerability scan of targets: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Penetration into targets: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Application­level manipulation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Client­side Java/ActiveX reverse engineering: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Physical penetration attempts: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Social engineering of people: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Will penetration test include internal network testing: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If so, how will access be obtained: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Are client/end­user systems included in scope: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If so, how many clients be leveraged: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is social engineering allowed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If so, how may it be used: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Are Denial of Service attacks allowed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Are Dangerous checks/exploits allowed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Primary Contact representing Target Organization

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Head of Penetration Testing Team

### Remote Access Policy

This Information Technology Remote Access Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides a standard for utilizing remote access into [Organization] corporate internal network.

#### 1.0) Overview

See Purpose.

##### 2.0) Purpose

The purpose of this policy is to define standards for connecting to [Organization] network from any host. These standards are designed to minimize the potential exposure to [Organization] from damages which may result from unauthorized use of [Organization] resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical [Organization] internal systems, etc.

#### 3.0) Scope

This policy applies to all [Organization] employees, contractors, vendors and agents with a [Organization]-owned or personally-owned computer or workstation used to connect to [Organization] network. This policy applies to remote access connections used to do work on behalf of

[Organization], including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to DSL, VPN, SSH.

#### 4.0) Policy

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

General access to the Internet for recreational use by immediate household members through [Organization] Network on personal computers is permitted. [Organization] employee is responsible to ensure the family member does not violate any [Organization] policies, does not perform illegal activities and does not use the access for outside business interests. [Organization] employee bears responsibility for the consequences should the access be misused. [Organization] Acceptable Use Policy details the actions that are acceptable and not acceptable for [Organization] computing devices to be utilized for.

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of [Organization] network:

* *Acceptable Encryption Policy*
* *Wireless Communications Policy*
* *Acceptable Use Policy*

#### 4.1) Requirements

* Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong passphrases as described in [Organization] Password Protection Policy and [Organization] Password Construction Policy. For information on creating a strong pass-phrase see the Password Policy.
* At no time should any [Organization] employee provide their login or email password to anyone, not even family members.
* [Organization] employees and contractors with remote access privileges must ensure that their [Organization]-owned or personal computer or workstation, which is remotely connected to [Organization] corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
* [Organization] employees and contractors with remote access privileges to [Organization] corporate network must not use non-[Organization] email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct [Organization] business, thereby ensuring that official business is never confused with personal business.
* Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
* Non-standard hardware configurations must be approved by [Organization], and [Organization] Information Security Manager must approve security configurations for access to hardware.
* All hosts that are connected to [Organization] internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers.
* Personal equipment that is used to connect to [Organization] networks must meet the requirements of [Organization]-owned equipment for remote access.
* Organizations or individuals who wish to implement non-standard Remote Access solutions to [Organization] production network must obtain prior approval from [Organization] Information Security Department.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Dual Homing | An Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures for implementing preventive security. |
| Split Tunneling | A computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. |

### Software Installation Policy

This Information Technology Software Installation Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides a reference document such that employees and personnel using [Organization] system and resources do not harm the system or affect other systems through installation of software directly or indirectly.

#### 1.0) 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 (covered in [Organization] Audit Policy), 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.

#### 2.0) Purpose

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

#### 3.0) Scope

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

#### 4.0) Policy

* Employees may not install software on [Organization] computing devices operated within [Organization] 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.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

### Vulnerability Management Policy

#### 1.0) Overview

[Organization]’s Information Security Department’s intentions for publishing the Vulnerability Management Policy is to ensure that any vulnerability is identified, responsibility for mitigation is assigned, proper logging and auditing of the vulnerability and remediation is performed, and future releases will not contain a similar or variant of the vulnerability.

Effective security is a team effort involving the participation and support of every LiveSafe 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.

#### 2.0) Purpose

The purpose of this policy is to provide Vulnerability Management guidance. Additionally, this policy provides direction to ensure that Federal regulations are followed, and corporate authority is granted to the Stakeholder Communication Implementation Lead (SCIL) and General Counsel for the notification of stakeholders when a vulnerability may place their data at risk,

#### 3.0) Scope

This policy applies to all [Organization] employees and affiliates.

#### 4.0) Policy

The Vulnerability Management Guidelines below provides details on how to identify and categorize vulnerabilities, who is responsible for mitigation, how to properly log and audit vulnerability and remediation, and the process to incorporate lessons learned for the DevOps team so that future releases will not contain a similar or variant of the vulnerability. This policy is in support of the specific NIST 800-53 R4 security controls that support vulnerability management, risk assessment, and risk remediation efforts are:

* Flaw Remediation (SI-2)
* Risk Assessment (RA-3)
* Vulnerability Scanning (RA-5)

##### 4.1) Identifying and Categorizing Vulnerabilities

[Organization] Vulnerability Management policy is modeled after the United States National Institute of Standards and Technology (NIST) publications NIST SP 800-40 R3 Guide to Enterprise Patch Management Technologies, and NIST SP 800-51 R1 Guide to Using Vulnerability Naming Schemes.

[Organization] subscribes to the US-CERT Alerts and Advisories and when notified of a vulnerability checks the Mitre Common Vulnerabilities and Exposures (CVE) to obtain the CVE (<http://cve.mitre.org>) particulars and also checks the NIST U.S. National Vulnerability Database (NVD) and the NIST Common Vulnerabilities Scoring System (<https://nvd.nist.gov/cvss.cfm>) to evaluate the impact of the vulnerability of [Organization] IS.

[Organization] also utilizes internal and external penetration testing and White Hat services and monitors the OWASP Top 10 (and others) to identify vulnerabilities that may not appear as a CVE, but still leave [Organization] exposed for potential exploit. In this case, the VP of Engineering and the DevOps team determine the CVSS score using the CVSS calculator (<https://www.first.org/cvss/calculator/3.0>).

Based on the CVE and CVSS score (http://www.cvedetails.com/cvss-score-distribution.php), the following classifications describe the severity levels that can be assigned to a vulnerability.

**Level Five (CVSS Score 9-10):** Urgent denotes a vulnerability through which an intruder can easily gain control at the administrator level of any affected host. This class of vulnerabilities poses the highest risk for a system-wide compromise of the IS.

Target Time to Remediate: 30 days

**Level Four (CVSS Score 7-9):** Critical denotes a vulnerability through which an intruder could gain access to the host at the administrator level or could possibly access Sensitive Information stored on the host. While this class of vulnerabilities is extremely serious, the risk of a breach or compromise is not as urgent as with a critical vulnerability.

Target Time to Remediate: 30 days

**Level Three (CVSS Score 5-6):** Serious denotes a vulnerability that may allow an intruder to gain access to specific information stored on the host, including security settings. While not immediately associated with a compromise of an affected host, these vulnerabilities allow intruders to gain access to information that may be used to compromise the host in the future.

Target Time to Remediate: 45 days

**Level Two (CVSS Score 3-5):** Medium Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

Target Time to Remediate: 60 days

**Level One (CVSS Score 1-3):** Minimal denotes vulnerabilities that do not pose an immediate threat to the host or the MSCP. These vulnerabilities refer mostly to weaknesses in a device that allow an intruder access to information that may be used in the future to compromise the host. Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Target Time to Remediate: 90 days

#### 4.2) Mitigation

The Senior VP of Engineering will review the vulnerability and CVSS scores and findings and assign a member of the DevOps team to research and present mitigation and remediation Courses Of Action (COA’s), along with an estimated time and cost to complete. The DevOps team will create a JIRA ticket and follow the normal bug fix and testing protocols in the Development environment to remediate the vulnerability, push through the Staging and then to Production as quickly as possible. The DevOps team will generate a Lessons Learned to document the root cause and review the MCSP code for any other potential future development efforts that may be affected.

#### 4.3) Logging Vulnerabilities And Remediation

The ISSM will log the Vulnerability notification, CVE, CVSS, and Time to Complete in the Plan Of Action and Milestones (POAM) and notify the ISSO. The ISSM will monitor the status of remediation through completion and update the POAM and notify the ISSO for final review and acceptance of the vulnerability remediation. The Monthly Security Audit will include the POAM item until the remediation is complete and closed. The ISSM will log the JIRA tickets in the POAM and Audit Logs.

#### 4.4) Lessons Learned

The DevOps team will present Lessons Learned to the ISSM, ISSO and all DevOps team members, and incorporate into the Secure Development Life Cycle documentation and processes.

#### 5.0) Compliance

[Organization] Information Security Department 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. Any exception to the policy must be approved by the LiveSafe Information Security Department in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Common Vulnerability Exposure (CVE) | Common Vulnerabilities and Exposures (CVE®) is a [dictionary](https://cve.mitre.org/cve/index.html) of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization’s security tools. If a report from one of your security tools incorporates CVE Identifiers, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem. |
| Common Vulnerabilities Scoring System (CVSS) | The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. |
| Exposure | An "exposure" is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.  CVE considers a configuration issue or a mistake an exposure if it does not directly allow compromise but could be an important component of a successful attack, and is a violation of a reasonable security policy.  An "exposure" describes a state in a computing system (or set of systems) that is not a vulnerability, but either:   * allows an attacker to conduct information gathering activities * allows an attacker to hide activities * includes a capability that behaves as expected, but can be easily compromised * is a primary point of entry that an attacker may attempt to use to gain access to the system or data * is considered a problem according to some reasonable security policy |
| National Vulnerability Database (NVD) | NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA). |
| Open Web Application Security Project (OWASP) | The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. |
| Vulnerability | A "vulnerability" is a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, OR availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety). |

### Wireless Communication Policy

This Information Technology Wireless Communication Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides guidelines for wireless communication and configuration of those clients to prevent threats from gaining access to network resources.

#### 1.0) 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.

#### 2.0) Purpose

The purpose of this policy is to secure and protect the information assets owned by [Organization] provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. [Organization] 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 [Organization] internal 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 [Organization] internal network.

#### 3.0) Scope

All employees, contractors, consultants, temporary and other workers at [Organization], including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of [Organization] must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a [Organization] network or reside on a [Organization] 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.

#### 4.0) Policy

##### 4.1) General Requirements

All wireless infrastructure devices that reside at a [Organization] site and connect to a [Organization] network, or provide access to information classified as [Organization] Confidential, or above must:

* Abide by the standards specified in [Organization] Wireless Communication Standard.
* Be installed, supported, and maintained by an approved support team.
* Use [Organization] approved authentication protocols and infrastructure.
* Use [Organization] 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) Isolated Wireless Device Requirements

All wireless infrastructure devices that provide access to [Organization] Confidential or above, must adhere to section 4.1 above (General Requirements). Isolated wireless devices that do not provide general network connectivity to [Organization] network must:

* Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with [Organization] 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 [Organization] corporate network, must conform to the Home Wireless Device Requirements as detailed in [Organization] Wireless Communication Standard.
* Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to [Organization] corporate network. Access to [Organization] corporate network through this device must use standard remote access authentication.

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| MAC Address | A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment |

### Wireless Communication Standard

This Information Technology Wireless Communication Standard is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides a standard specifying the technical requirements that wireless infrastructure devices must satisfy to connect to a [Organization] network.

#### 1.0) Overview

See Purpose.

#### 2.0) Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a [Organization] network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by [Organization] Information Security Manager are approved for connectivity to a [Organization] 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 [Organization] Information Security Manager approved support organization. Lab network devices must comply with the Lab Security Policy.

##### 3.0) Scope

All employees, contractors, consultants, temporary and other workers at [Organization] and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of [Organization], 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. [Organization] Information Security Manager must approve exceptions to this standard in advance.

##### 4.0) Standard

###### 4.1) General Requirements

All wireless infrastructure devices that connect to a [Organization] network or provide access to [Organization] Confidential, [Organization] Highly Confidential, or [Organization] 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.

###### 4.2) Lab and Isolated Wireless Device Requirements

* Lab device Service Set Identifier (SSID) must be different from [Organization] production device SSID.
* Broadcast of lab device SSID must be disabled.

##### 4.3) Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a [Organization] 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

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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

#### 7.0) Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| AES | Advanced Encryption Standard - An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm. |
| EAP-FAST | Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling |
| EAP-TLS | Extensible Authentication Protocol-Transport Layer Security |
| PEAP | Protected Extensible Authentication Protocol |
| SSID | Service Set Identification |
| TKIP | Temporal Key Integrity Protocol |
| WPA-PSK | WiFi Protected Access-Pre-Shared Key |

### Workstation Security Policy

This Information Technology Workstation Security Policy is one of the primary documents recommended by the National Institute of Standards and Technology (NIST) Risk Management Framework. The plan provides an outline of measures that should be taken to ensure that workstations within [Organization] are secured and guidelines are set to ensure security of information that reside on those workstations.

#### 1.0) Overview

See Purpose.

#### 2.0) Purpose

The purpose of this policy is to provide guidance for workstation security for [Organization] workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule “Workstation Security” Standard 164.310(c) are met.

#### 3.0) Scope

This policy applies to all [Organization] employees, contractors, workforce members, vendors and agents with a [Organization]-owned or personal-workstation connected to [Organization] network.

#### 4.0) Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information and that access to sensitive information is restricted to authorized users. Workforce members using workstations shall consider the sensitivity of the information that may be accessed and take actions to assist to minimize the possibility of unauthorized access. [Organization] will implement physical and technical safeguards for all workstations to restrict access to authorized users.

Appropriate measures include:

* Restricting physical access to workstations to only authorized personnel.
* Securing workstations (screen lock or log out) 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 [Organization] Password Policy.
* Complying with all applicable password policies and procedures. See [Organization] Password Policy for more information regarding proper password generation and security.
* Ensuring workstations are used for authorized business purposes only.
* Never installing unauthorized software on workstations. See [Organization] Software Installation Policy for more information regarding the proper methods and channels of installing software on [Organization] computing devices.
* Storing all sensitive information on network servers
* Keeping food and drink away from workstations in order to avoid accidental spills and resulting damage to workstations.
* 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 upon leaving a workstation to ensure unauthorized access, if it does happen, has less of an impact on business operations.
* 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 [Organization] Wireless Communication policy

#### 5.0) Compliance

[Organization] Information Security Manager will verify compliance to this policy through various methods, including but not limited to, periodic walkthroughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by [Organization] Information Security Manager in advance.

#### 6.0) Enforcement

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