MileStone

MILESTONE CONFIDENTIAL

Milestone IT Security Policy

Date:	05/01/2018
Owner:	Mitul Mehta
Created by:	Duke Tien
Department:	Information Technology

Document Version Control

Revision	Date	Author(s)	Change Summary
1	4/2/19	Duke Tien	Updated page 38: Customer's scoped data storing on all types of portable media/storage devices are prohibited
2	2/27/20	Duke Tien	Review
3	3/10/21	Mitul Mehta	Review
4	1/15/22	Mitul Mehta	Added the VPN Policy Change Font and format. Review
5	3/22/23	Mitul Mehta	Updated the change management metrics, Patch Management and Backup Policy
6	4/10/24	Mitul Mehta	Update password policy

Contents

Information Security Policy and Standards

Introduction

Storage of data on computers and servers and transfer across the network are paramount for day-to-day operations of Milestone, as is the case with most companies in today's day and age. Commensurate with that business necessity is the need for appropriate security measures.

The Information Security Policy (Policy) recognizes that not all departments within Milestone are the same and that data is used differently by different departments. The principles of academic freedom and the free exchange of ideas apply to this policy, and this policy is not intended to limit or restrict those principles. These policies apply to all departments within Milestone Inc.

Each department within Milestone should adhere to this policy to meet their information security needs. The Policy is written to incorporate current technological advances. The technology installed at some departments may limit immediate compliance with the Policy. Instances of non-compliance must be reviewed and approved by the Chief Information Officer or the equivalent officer(s).

Throughout the document, the terms *must* and *should* are used carefully. "Musts" are not negotiable; "should" are goals for Milestone. The terms *data* and *information* are used interchangeably in the document.

The terms *system* and *network* administrator are used in this document. These terms are generic and pertain to any person who performs those duties, not just those with that title or primary job duty. To illustrate, many employees are the system administrators for their machines.

Purpose of this Policy

By information security, we mean protection of Milestone's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purposes of the information security policy are:

To establish a company-wide approach to information security

To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of Milestone data, applications, networks, and computer systems

To define mechanisms that protect the reputation of Milestone and allow Milestone to satisfy its legal and ethical responsibilities about its networks' and computer systems' connectivity to worldwide networks

To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy

Responsibility

The chair of Milestone Technology Management Team (MTMT) is responsible for implementing this policy. MTMT, chaired by the Vice President of Technology, consists of the following teams:

1. IT Department
2. HR Department
3. Software and Development

MTMT must see to it that:

- The information security policy is updated regularly and published as appropriate
- Appropriate training is provided to data owners, data custodians, network and system administrators, and users
- Each department appoints a person to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

Members of MTMT are each responsible for establishing procedures to implement these policies within their areas of responsibility, and for monitoring compliance.

General Policy

Required Policies

- Milestone will use a layered approach of overlapping controls, monitoring, and authentication to ensure the overall security of Milestone's data, network, and system resources.

- Milestone will perform security reviews of servers, firewalls, routers, and monitoring platforms regularly. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Recommended Practices

- Vulnerability and risk assessment tests of external network connections should be conducted regularly. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.

- Education should be provided to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual, network administrator, system administrator, data

Data Classification Policy

It is essential that all Milestone data be protected. There are however, gradations that require different levels of security. All data should be reviewed periodically and classified according to its use, sensitivity, and importance. We have specified three classes below:

High Risk - Information assets for which there are legal requirements for preventing the disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA, PCI DSS, or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.

This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to Milestone if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

Confidential - Data that would not expose Milestone to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public - Information that may be freely disseminated.

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through Milestone.

- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.

- No Milestone-owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.

- Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its

- High-risk data must be encrypted during transmission over insecure channels.
- Confidential data should be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

Access Control Policy

- Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
- Where possible and financially feasible, more than one person must have full rights to any Milestone owned server storing or transmitting high-risk data. Milestone must have a standard policy that applies to user access rights. This will suffice for most instances. Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems should be achieved by individual and unique logins and should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
- Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. When limited access to Milestone-related documents or files is required specifically and solely for the proper operation of Milestone and where available technical alternatives are not feasible, exceptions are allowed under an articulated unit policy that is available to all affected unit personnel. Each such policy must be reviewed by the unit executive officer and submitted to the VP of Technology for approval. All users must secure their username or account, password, and system access from unauthorized use.
- All users of systems that contain high-risk or confidential data must have a strong password- the definition of which has been established by MTMT and is defined in chapter VI (Password Policy) of this document. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established by MTMT.

- Passwords must not be placed in emails unless they have been encrypted.
- Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.

- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.

- Users are responsible for the safe handling and storage of all Milestone authentication devices. Authentication tokens (such as a Secure ID card) should not be stored with a computer that will be used to access Milestone's network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing department so that the device can be disabled.

- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.

- Transferred employee access must be reviewed and adjusted as found necessary.

- Monitoring must be implemented on all systems, including recording login attempts and failures, successful logins and date and time of logon and logoff.

- Activities performed as administrator or Super-user must be logged where it is feasible to do so.

- Personnel who have administrative system access should use other, less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.

Virus Prevention Policy

- The willful introduction of computer viruses or disruptive/destructive programs into Milestone environment is prohibited, and violators may be subject to prosecution.

- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.

- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor's recommendations.

- Headers of all incoming data including electronic mail, must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.

- Where feasible, system or network administrators should inform users when a virus has been detected.

- Virus scanning logs must be maintained whenever an email is centrally scanned for viruses.

Intrusion Detection Policy

- Intruder detection must be implemented on all servers hosted at Azure Public Cloud

- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems, must be enabled.

- Server, firewall, and critical system logs should be reviewed frequently. Where possible, the automated review should be enabled, and alerts should be transmitted to the administrator when a serious security intrusion is detected.

- Intrusion tools should be installed where appropriate and checked regularly.

Internet Security Policy

- All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk.

- All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data is classified confidential.

System Security Policy

- All systems connected to the Internet should have a vendor-supported version of the operating system installed.

- All systems connected to the Internet must be current with security patches.

- System integrity checks of host and server systems housing high-risk Milestone data should be performed.

Acceptable Use Policy

Milestone must have a policy on appropriate and acceptable use that includes these requirements:

- Milestone computer resources must be used in a manner that complies with Milestone policies and State and Federal laws and regulations. It is against Milestone policy to install or run software requiring a license on any Milestone computer without a valid license.

- Use of Milestone's computing and networking infrastructure by Milestone employees unrelated to their Milestone positions must be limited in both time and resources and must not interfere in any way with Milestone functions or the employee's duties. It is the responsibility of employees to consult their supervisors if they have any questions in this respect.

- Uses that interfere with the proper functioning or the ability of others to make use of Milestone's networks, computer systems, applications, and data resources are not permitted.

- Use of Milestone computer resources for personal profit is not permitted except as addressed under other Milestone policies.

- The decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations. Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Auditors or security officers in the performance of their duties may also use them. They must not be used to monitor or track any individual's network activity except under special authorization as defined by campus policy that protects the privacy of information in electronic form.

Exceptions

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use which does not comply, but near-term future systems will, and are planned for;
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, units must develop a written explanation of the compliance issue and a plan for coming into compliance with Milestone's Information Security Policy in a reasonable amount of time. Explanations and plans must be submitted to Milestone VP of Technology or the equivalent officer(s).

Incident Response Policy

Purpose

Incident response capabilities are used to monitor for security incidents, determine the magnitude of the threat presented by these incidents, and to respond to these incidents. Without an incident response capability, the potential exists that, if a security incident occurs, it will go unnoticed and the magnitude of harm associated with the incident will be significantly greater than if the incident were noted and corrected.

Scope

This Incident Response Policy applies to all information systems and information system components of Milestone Internet Marketing. Specifically, it includes:

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

Policy

Incidents are prioritized based on the following:

- ❖ The criticality of the affected resources (e.g., Web server, user workstation)
- ❖ The current and potential technical effect of the incident (e.g., root compromise, data destruction).

Combining the criticality of the affected resources and the current and potential technical effect of the incident determines the business impact of the incident. For example, data destruction on a user workstation might result in a minor loss of productivity, whereas root compromise of a Web server might result in a major loss of revenue, productivity, access to services, and reputation.

Incident Reporting

All computer security incidents, including suspicious events, shall be reported immediately (orally or via e-mail) to the department Director of IT and department supervisor by the employee who witnessed/identified the breach.

Escalation

The department Director of IT and department supervisor needs to determine the criticality of the incident. If the incident is something that will have a serious impact, the VP of Technology, President, and CEO of Milestone Internet Marketing will be notified and briefed on the incident.

The VP of Technology, President, and CEO will determine if other agencies, departments, or personnel need to become involved in the resolution of the incident. Only the CEO, President, and VP of Technology will speak to the press about an incident.

Mitigation and Containment:

Any system, network, or security administrator who observes an intruder on Milestone Internet Marketing network or system shall take appropriate action to terminate the intruder's access. (Intruder can mean a hacker, botnet, malware, etc.) Affected systems, such as those infected with malicious code or systems accessed by an intruder shall be isolated from the network until the extent of the damage can be assessed. Any discovered vulnerabilities in the network or system will be rectified by appropriate means as soon as possible.

Eradication and Restoration

The extent of the damage must be determined, and the course of action planned and communicated to the appropriate parties.

Information Dissemination

Any public release of information concerning a computer security incident shall be coordinated through the office of VP of Technology.

The VP of Technology and his/her designee shall manage the dissemination of incident information to other participants, such as law enforcement or other incident response agencies. After consulting with the President and CEO, he/she shall coordinate dissemination of information that could affect the public, such as web page defacement or situations that disrupt systems or applications.

Ongoing Reporting

After the initial oral or e-mail report is filed, and if the incident has been determined to be a significant event (such as multiple workstations effected, root compromise, data breach, etc.), subsequent reports shall be provided to the VP of Technology and appropriate managers and President/CEO. Incidents such as individual workstations infected with malware are considered minor events and need not be followed up with a written report.

The incident reports shall be submitted within 24 hours of the incident. Some departments may be required to provide reports sooner in accordance with more stringent regulations. For example SSA and IRS requirements. If this is the case, the more stringent requirements are to be met.

A general report to the VP of Technology, President, and CEO shall contain the following:

- ✓ Point of contact
- ✓ Affected systems and locations
- ✓ System description, including hardware, operating system, and application software
- ✓ Type of information processed
- ✓ Incident description
- ✓ Incident resolution status
- ✓ Damage assessment, including any data loss or corruption
- ✓ Organizations contacted
- ✓ Corrective actions are taken
- ✓ Lessons learned

A follow-up report shall be submitted upon resolution by those directly involved in addressing the incident.

Review

After the initial reporting and notification, the Director of IT, department managers and VP of Technology shall review and reassess the level of impact that the incident created.

Policy Notification

Each Department Manager is responsible for ensuring that its employees are aware of where policies are located on websites. Departments Managers are also responsible for notifying employees of policy change or the creation of new policies that pertain to the department function.

Change Management Policy

Purpose

The purpose of this policy is to establish a uniform approach to technical change control. Information technology (IT) and business teams must manage system changes in a rational and predictable manner. Changes require planning, monitoring, testing, and follow-up evaluation to reduce the negative impact on the user community and to increase the value of information resources. This policy is not intended to be a statement of the current technical change control practices of Milestone Internet Marketing. It is a statement of goals and expectations. Meeting these goals and expectations are necessary to ensure the well-managed evolution of information technology systems.

Scope

The following non-exhaustive list depicts common types or reasons for system changes:

- User requests
- Vendor recommended/required changes
- Changes in regulations
- Hardware and software upgrades
- Acquisition/implementation of new hardware or software
- Hardware or software failures
- Changes or modifications to the infrastructure
- Unforeseen events
- Periodic Maintenance
- Application modifications and enhancements
- Patch deployment
- Network devices such as firewalls, routers, switches and access points

Policy

Information technology systems are subject to formal change control processes. Such processes provide a managed and orderly method by which changes are requested, tested, approved, communicated before implementation (if possible), and logged.

Attributes of a formal change control process/procedure include:

- Assignment of a technical change manager or change control team
- Written change requests submitted for all changes, both scheduled and unscheduled.
- Change requests receive formal approval before proceeding with the change.
- A testing plan is required to include IT and business representatives where appropriate.
- Customer notification is completed for each scheduled or unscheduled change.
- A post-change review is completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A changelog is maintained for all changes. The log should contain, but is not limited to:
    - Date of submission and date of the change
    - Owner and custodian contact information
    - Nature of the change
    - Indication of success or failure

Change control procedures for patches may require resources and processes very different from application change control, where for example, a formal change control board may be required. Departments should develop procedures and documentation that are appropriate to the change, level of risk, organizational structure, and audit requirements.

The following is a list of user roles and the responsibilities associated with those roles:

a. End-User/Functional User
    1. Submitting change requests
    2. Participating in user testing, pre-deployment testing, and post-deployment testing
    3. Sign off on the change where appropriate
    4. End/Functional User Management
    5. Verifying that change requests are valid
    6. Sign off on changes where appropriate

b. IT Staff are sometimes end-users, functional users, or functional user managers, and as such, have responsibility for following this policy.

c. IT Staff Technician Role – follows a prescribed change control process/procedure.

d. IT Management – overall responsibility for overseeing change control policy and processes, e.g., policy dissemination, oversight, and implementation approval of changes.

Change classifications:

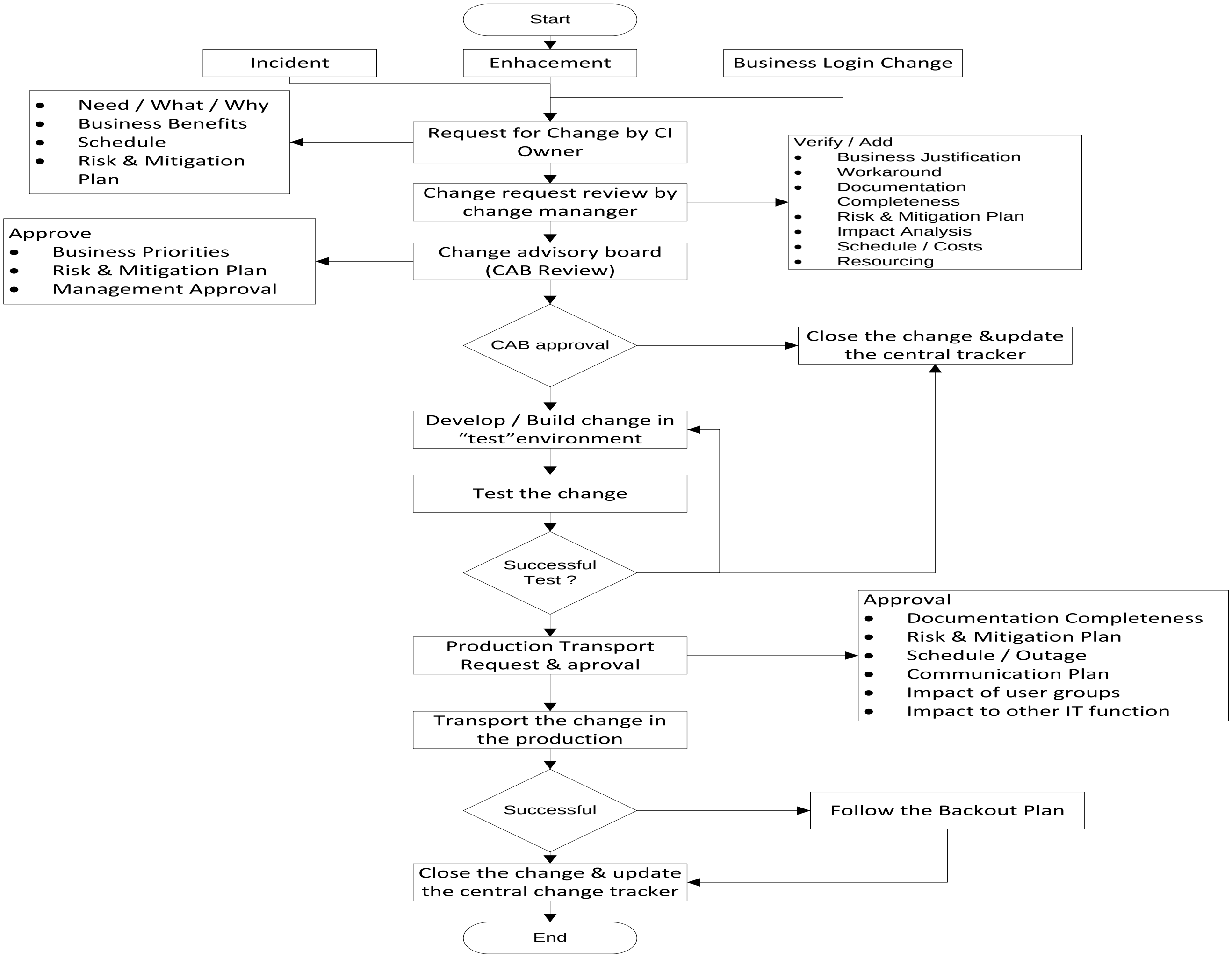
Tier Definition

Tier Classification	Description
Tier 1	Huge Business Impact (Revenue/Customer Impact) Many users affected Heavy transaction load
Tier 2	Medium Business Impact (Quiet a few Customers affected) Some users affected Medium transaction load
Tier 3	Low Business Impact Only a few customers affected Low transaction load

Change Type Definition

Type	**Description**	**Example**
Major	• New Service • Critical Hardware upgrade • Many customers impacted • 10 days Config/Development effort	• New Service introduction • Architectural Change • New Hardware
Minor	• New Features • Minor Config/Code Correction • < 10 days Config/Development effort • Service Pack/Major Patches • New Report/Enhancement	• Add-On Module/Card • Additional Switch/Router • Service Pack/Major Patches
Routine	• Defect Fixes • Urgent Fixes/Changes • Minor Patches	• Urgent Fixes/Changes • Hardware Reboot • System Parameter Changes • Minor Config Changes • Minor Patches

Change Management Flow Chart:



Policy Notification

Each department is responsible for ensuring that employees are aware of where policies are located on websites. Director of Client Services and VP of Technology are also responsible for notifying employees of policy change or the creation of new policies that pertain to the department function.

Wireless Network Policy

Purpose

Milestone Internet Marketing's computing and telecommunication networks, computing equipment, and computing resources are owned by Milestone and are provided to support day to day operation at Milestone.

Wireless communications networks use radio waves as a transport medium instead of copper cables to transmit voice and data signals. As such, they permit wireless-equipped communications devices to have mobile access to Milestone (wired) network wherever wireless communications access points are installed.

The purpose of this policy is to set the standard for network operation and security, specifically in the context of wireless network access. The configuration, installation, and maintenance of wireless communication network access point devices, if unmanaged, could result in severe interference with other network users and serious security risks.

Milestone IT Department defines the standards for the use of networks.

Scope

All employees, contractors, consultants, temporary and other workers at Milestone Internet Marketing, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Milestone Internet Marketing must adhere to this policy.

This policy applies to all wireless infrastructure devices that connect to a Milestone Internet Marketing network or reside on a Milestone Internet Marketing site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data.

Milestone Director of IT must approve exceptions to this policy in advance.

Policy

The Wireless Spectrum

a. Milestone regulates and manages all unlicensed radio frequencies in Milestone office.

b. Wireless equipment installed by Milestone uses either the FCC unlicensed 2.4 GHz Industrial/Scientific/Medical (ISM) band or the FCC 5.0 GHz Unlicensed National Information Infrastructure (U-NII) band.

c. Wireless equipment transmissions within the 2.4 GHz and 5.0 GHz bands conform to current IEEE 802.11 wireless LAN specifications.

d. Other wireless devices that also use the above-mentioned frequency bands, including but not limited to wireless LAN devices, cordless telephones, cameras, and audio speakers, will cause interference with Milestone-installed devices. As such, use of these devices is prohibited at Milestone office unless Milestone has tested the device and deemed it safe to use it within its network.

e. Milestone may restrict the use of any potentially interfering wireless radio device in Milestone-owned buildings and all outdoor spaces on the Milestone campus.

f. Employees who believe they have special wireless needs should contact Milestone's IT Department.

Wireless Network Operation and Security

1. The enterprise wireless infrastructure is managed by Milestone's IT Department as part of the Milestone's telecommunications network.

2. Milestone's IT Department will provide spectrum tuning, and general device management per access area according to wireless access device management standards.

3. Wireless networks will be segmented and treated as a "foreign/untrusted network" from a security standpoint. A firewall, router/switch VLAN technology, or similar technology will be employed to provide this segmentation.

4. Wireless users must be authenticated with unique user credentials.

5. Only authorized access points will be permitted. Unauthorized access points will be disabled.

6. Unauthorized traffic interception and/or bridging between the wired and wireless network is prohibited.

7. Applications supported over the wireless network will be limited, if this is necessary to provide an acceptable quality of service for all users.

8. No wireless spectrum interference or disruption of other authorized communications is permitted.

Enforcement

- Milestone's IT Department will enforce the *Wireless Network Policy* and establish standards, procedures, and protocols in support of the policy.
- An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Milestone Internet Marketing.
- Milestone's IT Department has the authority to disconnect network service or modify/enhance network security without notification in the event of law violation.

Review

- The VP of Technology has approved the *Wireless Network Policy* and Milestone's IT Department will periodically review the policy.

Patch Management Policy

Policy Statement

Milestone Internet Marketing will review, evaluate, and appropriately apply software patches in a timely manner. If patches cannot be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based upon the results of a risk assessment.

Rationale

To ensure the security of our network and protect Milestone's data, all computers and network devices must be maintained at vendor supported levels and critical security patches must be applied in a timely manner consistent with an assessment of risk.

This is a requirement of Milestone's Information Technology Security Program, and industry best practice guidelines.

Applicability of the Policy

This policy covers all servers, workstations, network devices, operating systems (OS), applications, and other information assets for which vendors provide system patches or security updates.

Definitions

- Network Devices - any physical component that forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.
- Network Infrastructure - Includes servers, network devices, and any other back-office equipment
- Patch - A fix to a known problem with an OS or software program. For the purposes of this document, the term "patch" will include software updates.
- OS - Operating System such Windows, Mac, Linux.
- Risk Assessment – An evaluation of the level of exposure to a vulnerability for which a patch has been issued.
- Update – a new version of software providing enhanced functionality and/or bug fixes.
- Vendor - any organization or individual(s) that do business with the Milestone Internet Marketing

Procedure

Patch Management and System Updates Policy:

a. System administrators will use automated tools, where available, to create a detailed list of all currently installed software on workstations, servers and other networked devices. A manual audit will be conducted on any system or device for which an automated tool is not available.

b. Systems and software will be evaluated to verify currency of patch and update levels and an analysis of vulnerabilities will be performed. Online resources such as US Computer Emergency Response Team (www.us-cert.gov/federal/) and the National Vulnerability Database (http://nvd.nist.gov) should be consulted in this process.

c. Specific guidelines for applying patches and updates will be developed and made available to system administrators.

Patch Management:

a. Automated tools will scan for available patches and patch levels, which will be reviewed as specified in the Patch Application Guidelines.

b. Manual scans and reviews will be conducted on systems for which automated tools are not available.

c. An informal risk assessment will be performed within 2 business days of the receipt of notification of patches. If a determination regarding the applicability of the patch or mitigating controls cannot be made in that time a formal risk assessment will begin.

d. Vendor supplied patch documentation will be reviewed to assure compatibility with all system components prior to being applied.

e. Where possible, patches will be successfully tested on non-production systems installed with most of critical applications/services prior to being loaded on production systems.

f. Successful backups of mission critical systems will be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching will be identified.

g. Patches will be applied during an authorized maintenance window in cases where the patch application will cause a service interruption for mission critical systems.

h. The production servers are getting patched every 3 Months while staging & UAT servers are getting patched every Month.

i. Patches will be prioritized and applied in accordance with Milestone Patch Application Guidelines.

j. Logs will be maintained for all system categories (servers, secure desktops, switches, etc.) indicating which devices have been patched. System logs help record the status of systems and provides continuity among administrators. The log may be in paper or electronic form. Information to be recorded will include but is not limited to: date of action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator's remarks.

k. In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels in effect before reloading.

l. In the event that a patch will not be applied due to incompatibility or risk assumption, precautions to mitigate the risk of exploitation to Milestone's network will be implemented and documented in the log.

Role & Responsibilities

a. Milestone IT staff is responsible for ensuring that information resources are maintained in compliance with Milestone patch management policies and procedures.

b. Administrators of systems not managed by Milestone IT staff are responsible for ensuring that their systems are maintained in compliance with Milestone patch management policies and procedures.

Contact

Questions related to the daily operational interpretation of this policy should be directed to:

Director Of IT
213-357-0565
Mitul Mehta (mitul.m@milestoneinternet.com)

Password Policy

Overview

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

Purpose

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

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

Policy

- A password should have the following characteristics:
    - At least eight characters.
    - Contain both upper and lower-case characters.
    - At least one digit and one punctuation character.
    - Must not be found in a dictionary or be a common use slang word.
    - Must not be a computer term, name, program, site, company name etc.
    - Must not contain the words "Milestone", "password" or any derivation.
    - Must not contain birthdays, phone numbers or other personal information.
    - Must not use word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Must not use any of the above spelt backwards.
    - Must not use any of the above preceded or followed by a digit (e.g. secret1, 1secret)
- Passwords must be changed from their initial default value the first time a new user logs in, and at least every six months thereafter.
- Use Active directory self-service portal to change login password – https://adss.milestoneinternet.com/authorization.do

- General password guidelines:

  - Passwords should never be sent via email or other forms of electronic communication.
  - A strong password should not be easy to guess, but it should be easy to remember, to prevent the necessity for the password to be written down. One way to do this is create a password based on a phrase or saying. For example, the phrase might be: "As sick as a dog" and the password could be “A5!kaD0g”.
  - A password that is used elsewhere (e.g. home internet, hotmail, etc.) should not be used as a Milestone password.
  - Passwords, or even the format of passwords, should not be shared with anyone. All users are responsible for the integrity and security of their password and are liable for any misuse of the password.
  - Passwords should not be written down, or stored on any computer (including laptops, smartphones, and tablet devices).
  - Passwords should be changed immediately if it is suspected that they have become known by another person.

- Passwords may be checked automatically to ensure they are sufficiently complex. Routine password auditing may be performed by the Milestone to ensure compliance with these standards.

- Password security is an individual responsibility and a failure to abide by this policy may result in disciplinary action.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Password cracking or guessing may be performed on a periodic or random basis by the Milestone IT Department or its delegates. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Audience

All people using Milestone’s network infrastructure, including employees, vendors, visitors and affiliates.

Server Security Policy

Purpose

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

Scope

This policy applies to server equipment owned and/or operated by Milestone, and to servers registered under any Milestone-owned internal network domain. This policy does not pertain to servers that are hosted at Rackspace's data center, which Milestone leases for its servers. This policy is specifically for equipment on the internal Milestone network. For secure configuration of equipment external to Milestone on the DMZ, refer to the *Internet DMZ Equipment Policy*.

Policy

Ownership and Responsibilities

All internal servers deployed at Milestone must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by VP of Technology. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by VP of Technology.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable

- Information in the corporate enterprise management system must be kept up-to-date.

- Configuration changes for production servers must follow the appropriate change management procedures.

General Configuration Guidelines

- Operating System configuration should be in accordance with industry security standard.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not uses root when a non-privileged account will do
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 2 weeks.
    - Weekly full tape backups of logs will be retained for at least 2 weeks.

- Security-related events will be reported to Director of IT, who will review logs and report incidents to VP of Technology. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

Compliance

- Audits will be performed on a regular basis by authorized personnel within Milestone.
- Audits will be managed by the internal audit group, in accordance with the Audit Policy. IT Department will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

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

Definitions

DMZ
De-militarized Zone. A network segment external to the corporate production network.

Server
For purposes of this policy, a Server is defined as an internal Milestone Server. Serves hosted at Rackspace, desktop machines and Lab equipment are not relevant to the scope of this policy.

Workstation Security Policy

Purpose

The purpose of this policy is to provide guidance for the security of computer workstations operated by Milestone Internet Marketing to ensure the security of information on the workstation and information to which the workstation may have access.

Scope

This policy applies to all employees of Milestone, its contractors, vendors and agents with a personal workstation connected to Milestone network.

Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected personal information and that access to sensitive information is restricted to authorized users.

Milestone will implement physical and technical safeguards for all workstations that access electronic protected sensitive information to restrict access to authorized users.

Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including personal information on network servers.
- Keeping food and drink away from workstations in order to avoid accidental spills.

- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents.
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- Mobile computing devices may not be removed from the premises prior to receiving Management approval.
- Remote access must be approved by the VP of Technology, President, or CEO. Remote access may be monitored by IT Department upon request.

Enforcement

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

Definitions

Workstations: laptops, desktops, PDAs, tablet computers, computer-based equipment containing or accessing information and authorized home workstations accessing Milestone network.

Identity Management Policy

Purpose and Scope

- The purpose of this policy is to describe the way digital identities are created, maintained, used, and terminated at Milestone

- This policy applies to all Milestone employees.

- This policy applies to the three ways that digital identities currently are maintained at Milestone: Active Directory and Card-Key.

Policy

Active Directory Domain Accounts

- The following types of individuals are eligible to receive an Active Directory domain user account for Milestone's network:
  - Current employees and staff members.
  - Current Milestone's Contractors and Consultants

- Active Directory domain usernames and initial passwords are assigned to users after they have signed an agreement, which, among other things, specifies that they have read and agree with the Policy on the Responsible and Ethical Use of Milestone Technology Resources.

  - Active Directory domain passwords:
    - Users must change their passwords when they first use their account.
    - Strong passwords are required (at least 8 characters, both upper and lower-case letters, one special character)
    - Passwords must be changed every 3 months

- Domain accounts are available only to users who are active employees, contractors and consultants at Milestone. Domain accounts will be disable and/or remove on the day that employee, contactor and/or consultant is no longer with Milestone.

Card-Key Access Accounts

- The Card-Key identifier is the same as the number on the card. These accounts are maintained by Pacific West Security.

Physical Security Policy

Overview

Managers, employees, records personnel, third party vendors and all others who connect to or handle Milestone networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by Milestone IT Department must explicitly state the more stringent requirements. Milestone IT Department shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

Purpose

Milestone office locations that include computers and other types of information technology resources must be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats. This includes but is not limited to; security doors, key entry areas, external doors that are locked from closing until opening of the building, locked and/or barred windows, security cameras, registration of visitors at entrances, and fire protection.

Information Security issues to be considered are:

- Unlawful access may be gained with the intent of theft, damage, or other disruption of operations.
- Unauthorized and illegal access may take place covertly (internal or external source) to steal, damage, or otherwise disrupt operations.
- Destruction or damage of physical space may occur due to environmental threats such as fire, flood, wind, etc.
- Loss of power may result in the loss of data, damage to equipment and disruption of operations.

Scope

This policy addresses threats to critical IT resources that result from unauthorized access to facilities owned or leased by Milestone, including offices, data centers and similar facilities that are used to house such resources.

All information resource facilities must be physically protected in proportion to the criticality or importance of their function. Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

Use of Secure Areas to Protect Data and Information

- Use physical methods to control access to information processing areas.
- These methods include, but are not limited to, locked doors, secured cage areas, vaults, ID cards, and biometrics.
- Restrict building assess to authorized personnel.
- Identify areas within a building that should receive special protection and be designated as a secure area. An example would be a server room.
- Use entry controls.
- Security methods should be commensurate with security risk.
- Ensure that physical barriers are used to prevent contamination from external environmental sources. For example: Water tight walls in flood zones. Proper ventilation in areas exposed to chemical vapors.
- Compliance with fire codes.
- Installation use and maintenance of air handling, cooling, UPS and generator backup to protect the IT investment within data rooms.

Physical Access management to protect data and information

- Access to facilities that house critical Milestone IT infrastructure, systems and programs must follow the principle of least privilege access. Personnel, including full and part-time staff, contractors and vendors' staff should be granted access only to facilities and systems that are necessary for the fulfillment of their job responsibilities.
- The process for granting physical access to information resources facilities must include the approval of the VP of Technology or Director of IT. Access reviews must be conducted at least quarterly, or more frequently depending on the nature of the

systems that are being protected. Removal of individuals who no longer require access must then be completed in a timely manner

- Access cards and keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.

- Security clearance for visitors. This could include, but is not limited to, a sign in book, employee escort within a secure area, ID check and ID badges for visitors.

Policy Notification

Department Manager/Director is responsible for ensuring that employees are aware of where policies are located on websites. Directors and/or VP Of Technology are also responsible for notifying employees of policy change or the creation of new policies that pertain to department function.

Role Change Policy

Please see Milestone Information Security Policy for more information.

Customer Data Handling Policy

Occasionally, it is necessary for customers to send data or source code to Milestone's customer support. Because this data may contain sensitive information, it is treated in a special way. Unless otherwise directed by a specific non-disclosure agreement, customer data is treated in the manner described below.

What is customer data?

Customer data is problem-specific information provided by the customer in electronic form for purposes of resolving product-related issues. This data may or may not include customer source code.

How does Milestone use customer data?

Customer data is used to resolve the specific issue submitted by the customer. In some cases, descriptive and procedural information provided by the customer may be used for regression testing and general explanation of product-related issues to other customers, for example in application notes published on our web site. Customer-specific information is never included in these cases.

Data transit & Store with Encryption?

Milestone is using Microsoft Platform Managed Key to store data at rest. We are using 256-bit AES encryption with 2048-bit for data encryption in transit.

How is customer data classified, handled and stored?

All customer data that is not open source or public is treated as confidential when it is received. Access to this information is restricted to a limited number of personnel on a "need to know" basis.

Customer's scoped data storing on all types of portable media/storage devices are prohibited.

When is customer data destroyed?

Customer data including source code, if submitted, is held on our servers for 6 months. After 6 months, the customer project data and source code are automatically deleted, except for any descriptive and procedural information referred to above which is not customer-specific, and which has been taken into use in regression testing and general explanation of product-related issues.

Remote Access Policy

Purpose

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

Scope

This policy applies to all Milestone employees, contractors and vendors with a Milestone-owned or personally-owned computer or workstation used to connect to the Milestone network. This policy applies to remote access connections used to do work on behalf of Milestone, 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, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

Policy

General

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

2. General access to the Internet for recreational use by immediate household members through the Milestone Network on personal computers is not permitted at all times. The Milestone employee is responsible to ensure the family member does not violate any Milestone policies, does not perform illegal activities, and does not access Milestone data at all. The Milestone employee bears responsibility for the consequences should the access is misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Milestone's network:
   a. Acceptable Encryption Policy
   b. Virtual Private Network (VPN) Policy
   c. Wireless Communications Policy

d. Acceptable Use policy

4. For additional information regarding Milestone's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., please contact Milestone IT Department.

Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

2. At no time should any Milestone employees provide their login or email password to anyone, not even family members.

3. Milestone employees and contractors with remote access privileges must ensure that their Milestone-owned or personal computer or workstation, which is remotely connected to Milestone's 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.

4. Milestone employees and contractors with remote access privileges to Milestone's corporate network must not use non-Milestone email accounts (i.e., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct Milestone business, thereby ensuring that official business is never confused with personal business.

5. Routers for dedicated ISDN lines configured for access to the Milestone network must meet minimum authentication requirements of CHAP.

6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

7. Non-standard hardware configurations must be approved by Remote Access Services, and Milestone IT Department must approve security configurations for access to hardware.

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

9. Personal equipment that is used to connect to Milestone's networks must meet the requirements of Milestone-owned equipment for remote access.

10. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Milestone production network must obtain prior approval from Milestone IT Department.

Enforcement

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

Definitions

TERM	DEFINITION
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus, the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or another Internet service provider (ISP). Being on a Milestone-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Milestone and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
Remote Access	Any access to Milestone's corporate network through a non-Milestone controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-Milestone network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Milestone's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

Split-tunneling	Simultaneous direct access to a non-Milestone network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Milestone's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

Logging and Security Monitoring Policy

Purpose

This policy establishes the uniform policy within Milestone for the auditing, logging, measurement, and monitoring of networks and automated information systems (AIS). This policy establishes minimum practices to ensure Milestone systems and networks are audited to maintain awareness of the operating environment, to detect indications of security problems, and to ensure Milestone AIS systems and networks are used for authorized purposes.

Scope

The provisions of this policy apply to all Milestone employees and contractor employees using or operating Milestone computer systems, as well as the systems and networks, and to contractor employees providing services to the Milestone by using Milestone AIS and networks. This policy applies to production AIS, servers and server applications only.

Policy

General Policy

It is Milestone's policy that audit trails shall be used for the following:

- Individual Accountability. Audit trails shall be used to support accountability by providing a trace of user actions.
- Reconstruction of Events. Audit trails shall be used to support after-the fact investigations of how, when, and why normal operations ceased.
- Intrusion Detection. Audit trails shall be designed and implemented to record appropriate information to assist in intrusion detection.
- Problem Identification. Audit trails shall be used as online tools to help identify problems other than intrusions as they occur.

All Milestone operational information technology (IT) systems shall enable audit and normal logging processes within the scope previously defined.

A. Contents of Audit Trail Records

An audit trail shall include sufficient information to establish what activity occurred and who (or what) caused them. Given the diversity of IT systems' capabilities and missions, the scope and contents of the audit trail shall balance security needs with performance needs, privacy, and costs.

The following list is representative of events that would provide an acceptable audit trail and is included in this policy as guidance.

- User login – unsuccessful, successful if feasible
- Server startup and shutdown
- Service startup and shutdown -- unsuccessful and successful, if feasible
- User account permission modifications -- unsuccessful and successful
- User account additions and deletions -- unsuccessful and successful
- IP address or hostname associated with a given event, if feasible
- Firewall rule base modification, if applicable -- unsuccessful and successful
- Software installation or removal -- unsuccessful and successful, if feasible

Audited events shall be documented in the appropriate system security plan or baseline configuration document of that operating system, network device, or application.

B. Audit Trail Security

Audit trails shall be protected from unauthorized access. The following precautions shall be taken:

- Control online audit logs. Access to online audit logs shall be strictly controlled.
- Separation of duties. Separation of duties between security personnel who administer the access control function and those who administer the audit trail shall be ensured.
- Protect confidentiality. Confidentiality of audit trail information shall be ensured.
- Audit logs shall be protected from accidental or malicious deletion and modification.
- Paper copies of audit logs shall have employed and distributed on a strictly need-to- know basis, shall be destroyed when no longer needed.

C. Audit Trail Reviews

Audit trails shall be reviewed as follows:

- For medium/highly critical servers on internal protected networks, on a weekly basis.

- For perimeter security intrusion detection systems on a daily basis, including firewall and IDS applications, daily.
- Following a known system or application software problem, a known violation of
- Existing policy by a user, or anomalous or suspicious system activity.

D. Automated Tools

To the maximum extent possible, audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, shall be used in real-time or near real- time. Audit analysis tools shall be used to help reduce the amount of information contained in audit trails, as well as to distill useful information from the raw data.

E. Monitoring of Milestone Network and AIS Activity

- Milestone networks and AIS shall be monitored for unauthorized or improper use.
- Unauthorized or improper use of the systems shall be investigated and, when appropriate, official sanctions shall be imposed as a result of such use. If criminal activity is discovered, system logs shall be provided to the appropriate law enforcement officials.
- The focus of network and AIS monitoring or auditing shall be predicated on identification and confirmation of behavior in violation of Milestone policy or federal law.
- Only authorized local network and system administrators, auditors, and/or investigators for diagnostic and troubleshooting purposes and monitoring of misuse or malicious network activity will use network packet analyzers, or devices that operate in promiscuous mode.

F. Employee Investigations

- Requests for an employee investigation can be made by: 1) the supervisor, or a superior in the management chain of the employee to be audited with the approval of Executive Management, 2) the Office of Human Resources, 4) Director of IT and 5) Milestone Executives (CEO, President & VP of Technology)
- A record shall be maintained of user investigation requests and results.

- Auditing can take place for any and all traffic on the network and AIS activity. All requests for log records related to employee misconduct (including Supervisors) shall be coordinated with VP of Operation & Technology approved by the President and/or CEO.

G. **Uniform Monitoring**

- Network and AIS monitoring shall only be used to monitor activity on a system-wide level without the targeting of any specific person(s) until any suspected unauthorized activity has been identified. To ensure the integrity and objectivity of the network monitoring function, segregation of duties shall be maintained.
- A user investigation report record shall be maintained for each individual investigation.
- Precautions shall be taken to prevent or decrease the risk of errors or irregularities with regard to data collection; identifying problems; and ensuring that the chain of evidence is preserved.
- No single individual shall have control over all phases of network monitoring.
- Approval for the collection, analysis, or use of the information gathered and the disclosure to law enforcement agencies, or other agencies outside the Milestone, shall be coordinated with VP of Technology and approved by the President and/or CEO.

H. **Employee Notification and Privacy Expectations.**

- Milestone employees and contractor employees shall be notified on logical access to a Milestone IT system through a warning message that must be agreed to or state that further use indicates consent to monitoring. This warning message will state that all IT systems may be monitored, and that unauthorized use will be grounds for disciplinary, civil or criminal proceedings.
- Milestone employees and contractor employees do not have a right, nor should they have an expectation, of privacy while using any Milestone IT system at any time, including accessing the Internet or using e-mail. To the extent that Milestone employees and contractor employees wish that their private activities remain private, they should avoid using Milestone IT systems, the Internet or e-mail. By using Milestone IT systems, Milestone employees and contractor employees give their consent to disclosing the contents of any files or information maintained using Milestone IT systems to authorized Milestone staff. In addition to access by authorized Milestone staff, data maintained on Milestone IT systems may be subject to the legal process of discovery and Freedom of Information Act (FOIA) requests.
- Milestone employees and contractor employees, by using Milestone IT systems, give implied consent to monitoring and recording with or without cause, including (but not limited to) their accessing the Internet or using e-mail. Any use of Milestone IT systems

is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

- Milestone employees and contractor employees shall not receive additional notification of specific monitoring actions of their usage unless the appropriate authority determines disciplinary action or criminal investigation is appropriate.

I. **Implementation**

Specific implementation details for this policy may be located in the appropriate system security plan of a given AIS or documented in the operating system baseline configuration document.

J. **Compliance**

- Prohibited uses of Milestone AIS resources can result in administrative, judicial or non- judicial punishment in accordance with federal law and civilian employee regulations.
- User Accounts shall be randomly audited to ensure compliance with established Milestone IT security standards. Milestone employee and contractor employee accounts shall be audited upon termination of employment and/or completion/termination of a contract.
- Audit trail information is subject to the Freedom of Information Act (FOIA).
- Milestone AIS, systems or applications that cannot meet established IT security standards shall be modified to remedy any deficiencies, where feasible. If compliance is not technically feasible then the System Owner of the AIS may defer compliance via a Plan of Action and an expected date of compliance or a waiver of this policy may be requested. For waiver details please refer to the Milestone IT Security Handbook or similar policy instruction.

Responsibilities

All Milestone employees and contractor employees shall be aware of and observe the Milestone policy regarding network and AIS audit, logging, measurement, monitoring. All Milestone employees and contractor employees shall adhere to this policy and refrain from any activity that might circumvent this policy.

System Owners, Information System Security Officers, and System Administrators shall implement the mandatory practices of this policy for all Milestone AIS, systems, or applications they are responsible for.

The Milestone IT Department shall:

- Log, monitor, and investigate possible security violations from activity involving access to and modification of sensitive or critical files.
- Review audit logs weekly for e-mail servers, medium and high criticality servers and hosts on the internal, protected network.
- Review audit logs from the perimeter security systems on a daily basis.
- Ensure the protection of system event logs with file-level permissions, segregation of duties, and all other safeguards commensurate with the highest level of sensitivity of the information resident on the system that the logs record data.
- When required, implement additional monitoring tools on critical servers as a supplement to the activity logging process provided by the operating system.

The Milestone IT Department shall ensure that all systems have current and effective IT security plans that accurately reflect system status.

The Milestone Information Technology Department shall:

- Maintain and update this policy and monitor compliance through the conduct of annual compliance reviews.
- Ensure communication of the policy to all Milestone employees and contractor employees and will ensure that IT security awareness and training programs address network and AIS audit, logging, measurement, and monitoring.
- Be responsible for monitoring of system user compliance with this policy as part of the periodic IT security self-assessment program or automated system audits.

Information Handling Policy

Please see Information Security Policy for more information

Business Continuity Policy

Introduction

Milestone is committed to providing the best possible experience to its customers and the best possible relationships with employees, shareholders and suppliers. To ensure the consistent availability and delivery of its products and services, Milestone has developed the following business continuity and disaster recovery (BC/DR) policy in support of a comprehensive program for BC, DR and overall business survivability.

Milestone, like any other company, is exposed to potential risks that could disrupt or destroy critical business functions and/or the production and delivery of Milestone products and/or services. Our strategy for continuing business in the event of an incident is to ensure the safety and security of all employees; and to continue critical business functions, production and delivery of products and services from predefined alternative sites.

Purpose and Scope

The purpose of the BC/DR policy is to ensure that all Company business activities can be kept at normal or near-normal performance following an incident that has the potential to disrupt or destroy the Company.

The scope of this policy is the entire Company, its subsidiaries, offices and employees in the U.S.A.

Statement of Policy

Each department in the Company is responsible for preparing current and comprehensive business continuity plans (BCP) for its operations. Certain departments, such as Information Technology (IT), are also responsible for disaster recovery plans (DRP) to ensure that any damage or disruptions to critical assets can be quickly minimized and that these assets can be restored to normal or near-normal operation as quickly as possible.

When a plan is completed, approved and implemented, each plan will include procedures and support agreements, which ensure on-time availability and delivery of required products and services. Each plan must be certified annually with the business continuity policy compliance process through the BC/DR Team.

Milestone recognizes the importance of an active and fully supported BC/DR program to ensure the safety, health and continued availability of employment of its employees and the production and delivery of quality goods and services for customers and other stakeholders.

Milestone requires the commitment of each employee, department and vendor in support of the activities required to protect Company assets, mission and survivability.

Policy Leadership

Anil Aggarwal, CEO, is designated as the corporate management liaison responsible for the BC/DR program. Resolution of issues in the development of, or support of, all BC/DR plans and associated activities should first be coordinated with the BC/DR Team and appropriate internal or external organizations before submitting to the corporate management liaison. The issue resolution process is defined in the following section.

Verification of Policy Compliance

BC/DR compliance verification is managed by the BC/DR Team with support from other relevant internal departments. Each plan must define appropriate procedures, staffing, tools and workplace planning activities necessary to meet compliance requirements. Plan templates have been developed to facilitate the plan development process, and these templates shall be used for all plans.

BC/DR Compliance Verification is required annually and is facilitated by the BC/DR Team. Waivers for temporary compliance verification may be given if a detailed written waiver request issued by the department manager is approved by the BC/DR Team corporate management liaison.

Penalties for Non-Compliance

In situations where a department does not comply with the BC/DR policy, the BC/DR Team will prepare a brief stating the case for non-compliance and present it to the BC/DR corporate management liaison for resolution. Failure to comply with BC/DR policies within the allotted time for resolution may result in verbal reprimands, notes in personnel files, termination and other remedies as deemed appropriate.

Disaster Recovery Plan

Disaster Recovery Plan is available separately upon request.

Backup Policy

Policy

This policy defines the backup policy for computers within Milestone organization which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

Purpose

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

Scope

This policy applies to all equipment and data owned and operated by the organization.

Definitions

- Backup - The saving of files onto magnetic tape, Cloud backup Vault or other mass storage media (including NAS and SAN devices) for the purpose of preventing loss of data in the event of equipment failure or destruction.

- Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

- Restore - The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

Backup Method and Timing

All critical product server data getting backed up with Azure Cloud backup as per the below mentioned schedule.

- Server Snapshot backup – 4 Hours
- Daily incremental backups
- 21 days retention
- Quarterly backup testing
- RPO 24 Hours
- RTO 2 Hours

Responsibility

The Director of IT will delegate a member of the IT department to perform regular backups.

Third Party Service Provider Policy

Selection Process

Milestone's Third-Party Service Providers (TPS Providers) are selected based on their level of service and experience in their particular area. All TPS Providers must have a minimum of three years' experience in their respective specialty along with the appropriate certifications for their field.

Milestone reevaluates its relationship with TPS Providers on an annual basis to determine whether the TPS Provider is meeting the expectations of Milestone and its clients.

Referral Process

Milestone makes recommendations to its clients based on their unique needs and requirements. Each TPS Provider is able to deliver a particular service to Milestone clients which cannot be provided by Milestone staff.

If a dispute arises between a client and a TPS Provider, Milestone will mediate to the best of its ability to resolve the conflict in a prompt and fair manner.

Ongoing communication between the client, the TPS Provider, and Milestone is critical to ensure a successful relationship. If at any time, you believe the level of service does not meet your expectation, you should inform Milestone as soon as possible. While Milestone cannot guarantee the quality of service provided, we make our best effort to assist our clients.

Compensation Arrangement

Under no circumstances does Milestone provide or receive compensation from its TPS Providers. There are no contracts between Milestone and its TPS Providers as to the type or level of service provided. Future referrals to TPS Providers are based on the quality of service to existing clients which ensures a high level of service to Milestone clients.

Employee Handbook

Please refer to Employee Handbook document.

Security Awareness Policy

Purpose

Effective information security requires a high level of participation from all members of Milestone. This policy defines responsibilities and roles for instilling information security awareness among all information resource owners, managers, service providers and users.

Scope

This policy affects all users of Milestone's information resources.

Policy Standards and guidelines

- All must be well informed of their responsibilities as Information Owners, Managers, Users, and Third-Party Service Providers.
- In cooperation with the training office, Milestone Director of IT is responsible for managing a Milestone training and awareness program for all employees of Milestone and for consulting with employees of Milestone on information security issues.
- Training classes and materials should be offered to instill the importance of appropriate information handling and to explain the implications of this Policy.
- Training should include specific information on the use of security precautions such as encryption, anti-viral tools, backup procedures, physical security and awareness of social engineering tactics.
- Milestone Director of IT is responsible for maintaining the Information Security Web site, which makes the information security resources described in this Policy available to Milestone community.
- Managers are responsible for seeing that their employees and faculty take advantage of available security awareness resources.
- Information Owners and Service Providers must become familiar with standard information security principles and procedures as they apply to the information resources under their care.

Definitions

Information resource:

This term includes information in any form and recorded on any media that is collected by or generated by any Milestone User. Information resources also include all computing, networking and communications equipment and software that are used for information processing and storage that are owned by Milestone or used by Milestone under license or contract.

Information Owners:
Information Owners are those employees of Milestone who have the primary responsibility for particular information. One becomes the Information Owner either by designation or by virtue of having acquired, developed, or created information resources for which no other party has information ownership

Users:
All employees of Milestone are "Users" of Milestone's information resources, even if they do not have responsibility for managing the resources. Users include: active employees, contractors, consultants, volunteers, and temporary employees.

Managers:
Managers are those who oversee daily operations and the activities of other employees or users in a Milestone office, unit or department.

Compliance

- All Milestone department heads and administrators are responsible for monitoring employee and faculty compliance with this policy.

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

Network Vulnerability Scanning and Penetration Testing

Brief Description:

Network scans of Milestone's systems and devices are conducted for the purpose of general security and vulnerability assessment. The policy grants appropriate members of the IT Department to coordinate and conduct *Vulnerability Assessments* and *Penetration Testing* against organizational assets.

Introduction:

Good security practices must be developed in conjunction with regular feedback on their effectiveness. One form of feedback can be produced using network-based security scanning tools. Regular scanning of devices attached to the network, to assess potential security vulnerabilities, is a *best practice* for managing a dynamic computing environment.

For critical enterprise systems or those dealing with sensitive data, additional testing methods to look deeper for more security vulnerabilities may be a *requirement* for compliance with laws, regulations, and/or policies. One of these methods is *Penetration Testing*, which is targeted at systems by IT security experts, and is typically performed at the request of Milestone's VP of Technology.

Scope:

All devices attached to the Milestone's network are subject to security vulnerability scanning and/or penetration testing. In today's changing environment, vulnerable and/or unprotected systems can easily be overlooked. Systems that are not properly managed can become a potential threat to the operational integrity of our systems and networks. Vulnerability scanning can be proactive, or reactive:

- Proactive security scanning allows for a meaningful assessment of system security against known risks, provides a roadmap of effective countermeasures for improving security, and also provides a simple quantification of assets.

- Reactive security scanning allows for threat quantification and assessment, accelerated damage control, and an assessment of systems against reasonable control measures during the repair/rebuild process.

Any critical enterprise systems of Milestone are subject to periodic vulnerability assessments. Any system dealing with information governed by laws, regulations, and/or

policies that require penetration testing are also covered. Other systems dealing with sensitive data may be submitted for penetration testing at the request of Milestone's VP of Technology, or at the recommendation of IT Department.

Penetration testing is a separate and distinctly different set of testing activities. Its primary focus is the exploitation (not just observation or assessment) of security vulnerabilities and therefore may be disruptive of operations (some exploits may cause operating systems or applications to "crash"). Penetration testing is most beneficial when executed after an Assessment has been performed and the issues found by that Assessment have been remediated.

Policy Statement:

Multiple levels and types of network security scanning are utilized by Milestone, and are managed as services by IT Department:

1. *Focused Scan*-- Low-level scans for basic service-tracking purposes will be conducted on all networks in Milestone's network. In addition, specialized scans to target specific problems posing a threat to Milestone's systems and networks or to correlate interrelated network-based vulnerabilities will be conducted on an ad-hoc basis. Focused scans are not typically advertised.

2. *Recurring Group Scan* – Groups of systems or departments identified as critical to Milestone, or that might subject Milestone to heightened risk will be subject to frequent, in-depth security scans. Any department can join the recurring group scan service upon request. Scan schedules are arranged with IT Department.

3. *Ad Hoc Scan* – Before a new system is put into service, it is recommended that a network security scan be conducted for the purposes of identifying potential vulnerabilities. Scans may be requested by system administrators at any time, as frequently as necessary to maintain confidence in the security protections being employed. Any system identified in conjunction with a security incident, as well as any system undergoing an audit may be subject to a network security scan.

4. *Penetration Test* - All penetration testing of Milestone systems must be arranged by Director of IT and coordinated through VP of Technology. Penetration testing is typically conducted over a period of several weeks, with regular feedback to VP of Technology if issues are identified.

Due to the more intrusive nature of a penetration test, and to better manage risks associated with such tests, a signed non-disclosure agreement and confidentiality agreement is required prior to commencing the penetration test

Penetration testing may be performed by any qualified service provider approved by VP of Technology.

High-risk issues must be remediated in a timely manner, work toward implementing compensating controls to reduce risks highlighted in the report(s).

Authorized scanning system includes, but is not limited to, periodic scans performed by Alert Logic

VPN Access Policy

Purpose

Virtual Private Network (VPN) service at Milestone is managed and provided by Milestone IT Team for members of the milestone employee and registered guests who require remote and secure access to Milestone's IT resources like file servers, print servers, software licensing and various web-based services when at home or traveling. In an effort to ensure the security and integrity of the service, certain requirements and guidelines must be met by the administrators and users of this service. The Virtual Private Network (VPN) service provides IT Team strongly recommends you use the VPN connection when connecting to Milestone resources over any unsecured (open or public) wireless network.

Intended Use

VPN access is provided for the Milestone Employee by Milestone IT Team provided that users adhere to all established policies relating to the use of the Milestone network and associated technology resources as well as applicable local, state and federal laws. Remote computers attaching to the VPN become an extension of the Milestone data network and are therefore subject to the same network use guidelines and policies extended to any other host on the network.

Usage Policy

VPN access will require authentication by user account/password and all traffic will be encrypted using standard protocols. All authentication attempts will be logged.

It is the responsibility of each VPN user that they do not allow any other individual to use their account to access the VPN.

If any violation of policy occurs, Milestone Internet IT Team may take any necessary step in ensuring the security of the VPN and the greater network. This may include temporary suspension of accounts and/or network access.