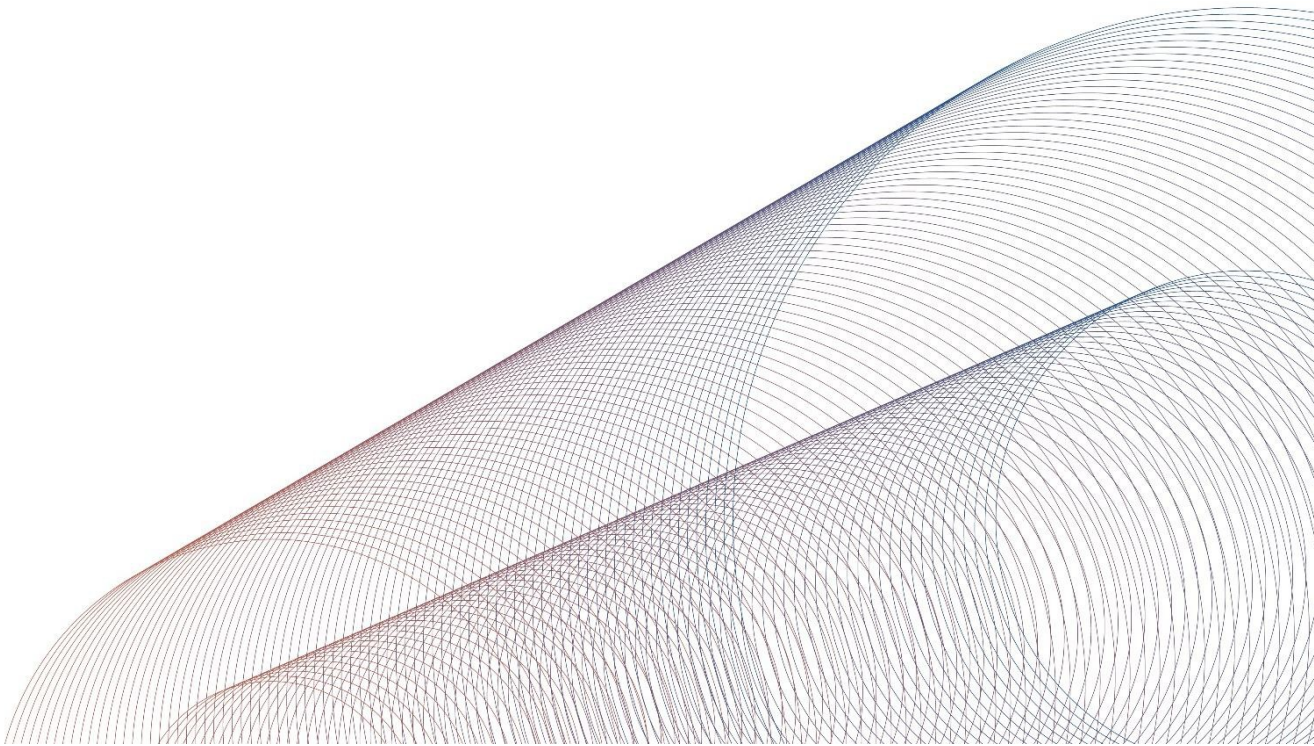
SitusAMC

IT Handbook

May 2021



REALIZING
OPPORTUNITIES
IN REAL ESTATE®

SitusAMC.com

Table of Contents

1. Acceptable Use

Overview

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

All SitusAMC systems, including but not limited to servers, laptops, desktops, operating systems, software, storage media, and network accounts providing electronic mail are property of SitusAMC. These systems are to be used for business purposes in serving the interests of the company, and of our clients in the course of normal business operations.

Effective security awareness is a team effort involving the participation and support of every SitusAMC employee, as well as SitusAMC contractors, consultants, temporary employees, and other workers at SitusAMC, including all personnel affiliated with third parties who deal with SitusAMC information and/or SitusAMC information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

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

Scope

This policy applies to employees, as well as SitusAMC contractors, consultants, temporary employees, and other workers at SitusAMC, including all personnel affiliated with third parties who deal with SitusAMC information and/or information systems. This policy applies to all equipment that is owned, leased or managed by SitusAMC.

Policy

General Use and Ownership

1. Access to and use of any and all SitusAMC systems and equipment is a privilege granted to each employee by SitusAMC management, which may be revoked, at any time, for any reason or no reason, at the company's sole discretion. All systems and equipment are meant to support, provide, and promote the goals and the mission of SitusAMC. Refer to SitusAMC's Information Security Policy for more information on this topic.
2. SitusAMC requires any information that it considers sensitive or vulnerable to be encrypted. For guidelines on information classification, see SitusAMC's Data Classification & Handling Guidelines contained within the Information Security Policy.
3. At any given time, SitusAMC systems are subject to monitoring, for security and network purposes by appropriate Information Security staff.
4. Loss, theft or damage to any SitusAMC equipment must be reported to your supervisor and the IT Departmentimmediately via email, to servicedesk@situsamc.comno later than 24 hours of becoming aware of the loss, theft or damage.

5. If SitusAMC equipment is stolen, the user must initiate a police report and provide a copy of said report to servicedesk@situsamc.com. Upon receipt of the report, a service desk ticket will be created on behalf of the employee for a replacement to be issued.
6. If SitusAMC equipment or property is negligently handled and damaged, or is lost as a result of negligent actions, in addition to SitusAMC pursuing disciplinary action as a result of violating this Policy, SitusAMC may also determine that the employee is responsible for paying the comparable equipment replacement cost, and will take such steps accordingly.
7. Failure to return SitusAMC equipment or property upon termination of employment, or upon company request, may be considered theft. In such a case, SitusAMC reserves all its legal rights, and may elect to pursue collection activities and/or initiate legal proceedings, where legally permissible.

Security and Proprietary Information

1. In accordance with the SitusAMC Information Security Policy and SitusAMC Privacy Policy, employees should take all necessary steps to prevent unauthorized access to sensitive information.
2. Employees are prohibited from sharing accounts and should keep their passwords secure. Passwords will be changed at minimum every 90-days.
3. Social media postings by employees to newsgroups, forums, or social media platforms, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SitusAMC. Before posting any data referencing SitusAMC or its subsidiaries to publicly accessible locations such as social media sites, the data or content must first be reviewed by SitusAMC Legal and must be classified as "Public".
4. Employees must use extreme caution when opening e-mail and their attachments received from unknown senders or external email addresses. These types of emails may contain malware, spyware, viruses or be a form of phishing/whaling.

Unacceptable Use

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

The following activities listed below are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. The lists below are not exhaustive and attempt only to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The Following Activities are Strictly Prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SitusAMC.
2. Revealing account passwords to others or allowing use of your account by others. This includes family and other household members when work is being conducted at home.
3. Using a SitusAMC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the employee's local jurisdiction.
4. Making fraudulent offers of products, items, or services originating from any SitusAMC account.
5. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port or vulnerability scanning is expressly prohibited unless prior notification and approval from SitusAMC Information Security (InfoSec) is received.
8. Circumventing user authentication or security of any host, network or account.
9. Copying any confidential data outside the confines of the SitusAMC network, including sending information to your personal email or personal cloud devices, without proper documented authorization from IT or InfoSec.
10. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network.
11. Providing information about, or lists of, SitusAMC employees to parties outside SitusAMC without SitusAMC's prior, written approval from Legal or InfoSec.
12. Employees are prohibited from connecting personally owned devices to SitusAMC network systems via a connection (wired, wireless or otherwise) at any SitusAMC office without proper documented authorization from IT or InfoSec.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or instant message, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Social Networking

In accordance with the SitusAMC Employee Handbook, employees may not post on a blog or web page or participate on a social networking, Twitter or similar site during working time or at any time with Company equipment or property, unless authorized to do so as part of his/her position with SitusAMC.

Enforcement

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

2. Clean Desk Policy

Overview

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

Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our clients and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/ 27002 compliant, but it is also part of standard basic privacy controls.

Scope

This policy applies to all SitusAMC employees and subsidiaries.

Policy

Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

Computer workstations must be locked when workspace is unoccupied.

File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

At the end of each work day, any restricted or sensitive information must be removed from employee desks and placed in the SitusAMC-provided secure shred bins for disposal.

Whiteboards containing Restricted and/or Sensitive information should be erased at the end of each day.

Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer or office.

All printers should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

Policy Compliance

Compliance Measurement

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

Exceptions

Any exception to the policy must be approved by the InfoSec team in advance. Exception request forms can be obtained by emailing servicedesk@situsamc.com.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with SitusAMC.

3. Password

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of SitusAMC's entire corporate network. As such, all SitusAMC employees (including contractors, consultants, temporary employees, and other workers at SitusAMC, all personnel affiliated with third party's contractors and vendors with access to SitusAMC 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 supports SitusAMC systems.

Policy

All default system-level users/passwords (e.g., root, enable, admin, domain admin, application administration accounts, etc.) must be disabled unless an exception is granted by InfoSec.

All production system-level passwords must be part of the SitusAMC administered global password management database.

All user-level passwords (e.g., email, computer, etc.) must be changed at least every 90 days.

User accounts that include system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

For new-hires and delivery of encrypted documents, separate emails will be sent with one email containing the UserID or document and a separate (second) email with the password. A single communication shall not contain both UserID/document and password.

All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

General Password Construction Guidelines

Passwords are used for various purposes at SitusAMC, and all employees should be aware of how to create strong passwords.

- Strong passwords will have the following characteristics within the SitusAMC network:
  - At least ten alphanumeric characters long.
  - Contain both upper and lower case characters (e.g., a-z, A-Z)
  - Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%A&*()_+|— =V{}[]:";'<>?,./)

- Should not contain a word in any language, slang, dialect, jargon, etc.
- Should not be based on personal information, such as names of family, etc.
- Should never be written down or stored on-line.

Password Protection Standards

Do not use the same password for SitusAMC accounts as for other non-SitusAMC access (e.g., personal email account, benefits, etc.). Where possible, don't use the same password for various SitusAMC access needs. For example, select one password for Active Directory and a separate password forthe benefits website.

Do not share SitusAMC passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential SitusAMC information.

Below is a List of "Don'ts":

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

If someone demands a password, refer them to this document, inform your direct supervisor or contact servicedesk@situsamc.com or call 888-748-8773. helpdesk@situsamc.com.

Do not use the "Remember Password" feature of applications or utilize form-completion features included within browsers. (e.g., Internet Explorer, Chrome andFirefox).

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smart devices (iPhone, Android)) without encryption.

If an account or password is suspected to have been compromised, report the incident to your manager, notify IT at servicedesk@situsamc.com and change all system passwords.

Application Development Standards

In accordance with the SitusAMC Change Management Policy, all application developers must ensure their programs contain the following security precautions.

Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Use of Passwords and Passphrases for Remote Access Users

Access to the SitusAMC Networks via remote access must include dual factor authentication (DFA). Employees authorized to work remotely must have a smart device (smart phone, tablet, etc.) to install software based DFA applications.

Passphrases

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

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." All of the rules above that apply to passwords also apply to passphrases.

Enforcement

Any 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 SitusAMC.

4. Email Use

Purpose

To ensure the public image of SitusAMC is not harmed in any way when transmitting email from SitusAMC to clients and the general public.

Scope

In conjunction with the SitusAMC InfoSec Policy and SitusAMC Employee handbook, this policy covers appropriate use of any email sent from a SitusAMC email address and applies to all employees, contractors, consultants, temporary employees, and other workers at SitusAMC, including all personnel affiliated with third parties operating on behalf of SitusAMC.

Policy

Prohibited Use

The SitusAMC email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any SitusAMC employee should report the matter to their supervisor immediately.

Personal Use

Only authorized employees are permitted to email outside the SitusAMC network/domain. In general, personal email usage is restricted unless approved as part of normal business functions. If granted use, limited personal email usage is allowed if it does not hinder performance of job duties or violate any other Company policy.

Monitoring

SitusAMC employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. SitusAMC may monitor messages without prior notice.

Enforcement

Any 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 SitusAMC.

Definitions Term and Definitions

Email - The electronic transmission of information through a mail protocol such as SMTP or IMAP. The organization subscribes to Microsoft's Office 365 platform, which utilizes Microsoft Outlook as the company-approved email application.

5. Anti-Virus

Purpose

SitusAMC has established baseline requirements which must be met by all computers connected to SitusAMC workstation networks to ensure effective virus detection and prevention.

Scope

This policy applies to all workstation computers in a SitusAMC office and any computer connecting to SitusAMC's network. This includes, but is not limited to, desktop computers, laptop computers, servers and any device capable of containing a virus.

Policy

All SitusAMC PC-based workstation computers must have SitusAMC's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to disable company approved anti-virus programs is prohibited, in accordance with the Acceptable Use Policy.

Enforcement

Any 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 SitusAMC.

6. Phone System and Voicemail Acceptable Use

Purpose

In order to protect the integrity of the public image of SitusAMC, and in a commitment to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly, this phone system and voicemail use policy outlines actions that must be taken by all employees to ensure security of company phone correspondence.

Scope

This policy covers appropriate use of the SitusAMC phone system and voicemails left to individuals from a phone owned by SitusAMC, as well as the security policies for voicemails. This policy applies to all employees, contractors, consultants, temporary employees, and other workers at SitusAMC, including all personnel affiliated with third parties operating on behalf of SitusAMC.

Policy

Prohibited Use

The SitusAMC phone system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, national origin, or other protected group. Employees who receive any voicemails with this content from any SitusAMC employee should report the matter to their supervisor immediately.

Personal Use

Using a reasonable amount of SitusAMC resources for personal phone calls is acceptable (other than personal international phone calls). Using SitusAMC resources for any personal work interests unrelated to the company will not be tolerated; this includes, but is not limited to, freelance work or employment with another organization.

Security

For every employee assigned a voicemail inbox by the company, it is a requirement that all voicemail boxes have passwords. Users must keep their voicemail password safe at all times; under no circumstances should an employee ever divulge their password information to another employee. If a password is forgotten, it is the employee's responsibility to notify their supervisor immediately.

No SitusAMC employee shall leave voicemail messages that contain sensitive or restricted information, unless absolutely necessary in the employee's reasonable judgment. In no event should a voicemail message result in an unauthorized disclosure.

Monitoring

SitusAMC employees shall have no expectation of privacy in anything they store or say on the company's phone system. SitusAMC may monitor phone calls, phone usage, and voicemail messages without notice.

Enforcement

Any 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 SitusAMC.

Definitions

Voicemail

A message left on an individual's phone in the event of the individual being unable to be at the phone.

Sensitive Information

Information is considered sensitive if it can be damaging to SitusAMC or its clients' reputation or market standing.

Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to people, both inside and outside SitusAMC, who do not have a need to know that information.

7. Remote Access

Purpose

The purpose of this policy is to define standards for connecting to SitusAMC's network from any host. These standards are designed to minimize the potential exposure to SitusAMC from damages which may result from unauthorized use of SitusAMC resources. Damages include the loss of sensitive, company, or client/third-party confidential data, intellectual property, reputational damage, damage to critical SitusAMC internal systems, etc.

Scope

In conjunction with the SitusAMC InfoSec Policy, this policy applies to all employees, contractors, consultants, temporary employees, and other workers at SitusAMC, including all personnel affiliated with third parties operating on behalf of SitusAMC with a SitusAMC- owned or personally-owned computer or workstation used to connect to the SitusAMC network. This policy applies to remote access connections used to do work on behalf of SitusAMC, including reading or sending email and viewing intranet web resources.

Policy

General

1. It is the responsibility of SitusAMC employees, contractors, vendors and agents with remote access privileges to SitusAMC's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to SitusAMC.
2. General access to the Internet for recreational use by immediate household members through the SitusAMC Network on personal computers is not permitted at any time. The SitusAMC employee is responsible to ensure the family member does not violate any SitusAMC policies, does not perform illegal activities, and does not access SitusAMC owned assets. The SitusAMC employee bears responsibility for the consequences if assets are misused.
3. For additional information regarding SitusAMC's remote access connection options contact your supervisor or the IT Service Desk (servicedesk@situsamc.com).

Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via dual factor authentication (DFA). In order to obtain DFA, employees are required to obtain their own smart device at their own expense for downloading DFA applications.
2. At no time should any SitusAMC employee provide their login or email password to anyone.
3. SitusAMC employees and contractors with remote access privileges must ensure that their SitusAMC- owned or personal computer or workstation, which is remotely connected to SitusAMC'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. SitusAMC employees and contractors with remote access privileges to SitusAMC's corporate network must not use non-SitusAMC email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct SitusAMC business, thereby ensuring that official business is never confused with personal business.
5. Reconfiguration of a equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
6. All hosts that are connected to SitusAMC internal networks via remote access technologies must use the most up-to-date anti-virus software.
7. When permitted, personal equipment that is used to connect to SitusAMC's networks must meet the requirements of SitusAMC-owned equipment for remote access.

Enforcement

Any 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 SitusAMC.

Definitions

Remote Access

Any access to SitusAMC's corporate network through a SitusAMC owned or non-SitusAMC controlled network, device, or medium.

VPN Virtual Private Network (VPN)
VPN is a method for accessing a remote network via a secure, encrypted tunnel through the Internet.

Split Tunneling

Simultaneous direct access to a non-SitusAMC network (such as the Internet, or a home network) from a remote device while connected into SitusAMC's corporate network via a VPN tunnel.

8. Virtual Private Network (VPN)

Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or SSL/TLS Virtual Private Network (VPN) connections to SitusAMC's corporate network.

Scope

This policy applies to all employees, contractors, consultants, temporary employees, and other workers at SitusAMC, including all personnel affiliated with third parties operating on behalf of SitusAMC and utilizing VPNs to access the SitusAMC network. This policy applies to implementations of VPN that are directed through any network appliance.

Policy

Approved SitusAMC employees and authorized third parties (clients, vendors, etc.) may utilize the benefits of VPNs, which is a "user managed" service.

Additionally:

1. It is the responsibility of employees and authorized third parties with VPN privileges to ensure that unauthorized users are not allowed access to SitusAMC internal networks.
2. VPN use is to be controlled using dual factor authentication (DFA) with a one-time password via a smart device.
3. When actively connected to the corporate network, the VPNs may force all traffic to and from the PC over the VPN tunnel; therefore, all other traffic may be dropped.
4. Dual (split) tunneling is not permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by SitusAMC IT Staff.
6. All computers connected to SitusAMC internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard. In addition, all computers must also be running the most updated firewall sets for Windows Firewall.
7. VPN users will be automatically disconnected from SitusAMC's network after ninety minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN connection is limited to an absolute connection time of 24 hours.
9. Only SitusAMC-approved VPN clients may be used. Personal VPN clients which masks the location of the user could alert IT/InfoSec and trigger an account lock down due to suspicious activity. As such, personal VPN's are not authorized to be used when connecting to SitusAMC issued accounts/networks.

Enforcement

Any 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 SitusAMC.

9. Wireless Communication

Overview

The purpose of this policy is to secure and protect the information assets owned by SitusAMC. SitusAMC provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. SitusAMC grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to SitusAMC's network.

Scope

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

InfoSec must approve any exceptions to this policy in advance. To obtain an exception request, email infosec@situsamc.com.

Policy Statement

General Network Access Requirements

All wireless infrastructure devices that reside at a SitusAMC site and connect to a SitusAMC network, or provide access to information classified as SitusAMC Confidential, SitusAMC Highly Confidential, or SitusAMC Restricted must:

1. Be properly configured/secured, using 802.1x w/ RADIUS.
2. Be installed, supported, and maintained by the IT Department.
3. Use SitusAMC approved authentication protocols and infrastructure.
4. Use SitusAMC approved encryption protocols.
5. Maintain a hardware address (MAC address) that can be registered and tracked.
6. Not interfere with wireless access deployments maintained by other support organizations.

Workstation and Isolated Wireless Device Requirements

All workstation wireless infrastructure devices that provide access to SitusAMC Confidential, SitusAMC or SitusAMC Restricted information must adhere to the Information Security Policy.

Enforcement

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 SitusAMC.

10. Removable Media

Overview

In accordance with the SitusAMC InfoSec Policy, SitusAMC's intent in publishing a Removable Media Policy is to control access to media devices. Removable media has been known to be the source of malware which is directly tied to the loss of sensitive information in many organizations.

Purpose

To minimize the risk of loss or exposure of sensitive information maintained by SitusAMC and to reduce the risk of acquiring malware infections on the computers and networks operated by SitusAMC.

Scope

This policy covers all computers and servers operating on SitusAMC's network.

Policy

Only approved SitusAMC staff may only use removable media. SitusAMC removable media may not be connected to or used in computers that are not owned or leased by SitusAMC without explicit documented permission of InfoSec. Sensitive information should never be stored on removable media unless it's a requirement in the performance of assigned duties or when providing information required by other state or federal agencies. When sensitive information, e.g. cardholder data, account numbers, and Social Security numbers, is stored on removable media, it must be encrypted in accordance with the SitusAMC InfoSec Policy. Exceptions to this policy may be requested on a case-by-case basis to InfoSec and have senior management approval. To obtain an exception request, email infosec@situsamc.com.

Enforcement

Any 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 SitusAMC.

Definitions

Removable Media

Any Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices, cell phones and other smart devices; removable hard drives; optical disks such as CD and DVD drives; and any commercial software disks not provided by SitusAMC.

Encryption

A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Sensitive Information

Information which, if made available to unauthorized persons, may adversely affect SitusAMC, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers, financial information, and client information.

Malware

Software of malicious intent/impact such as viruses, worms, and Spyware.

11. Technology Equipment Disposal

Overview

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

Purpose

This policy has been developed to define the requirements for proper disposal of technology equipment at SitusAMC.

Scope

This policy applies to all technology equipment owned, leased or managed by SitusAMC.

Policy

Technology Equipment Disposal

1. When technology assets have reached the end of their useful life, they will be sent to the St. Petersburg, FL Information Technology office for proper disposal.
2. The Information Technology department will securely erase and shred all storage mediums in accordance with current industry best practices.
3. The Information Technology department will ensure all assets are disposed of and receive a certificate of destruction, in compliance with SitusAMC's InfoSec Policy.
4. Prior to leaving SitusAMC premises, all equipment must be removed from the Information Technology inventory system.

Ramifications

Failure to properly dispose of technology equipment can have several negative ramifications to SitusAMC including fines, negative client and/or public perception and costs to notify constituents of data loss or inadvertent disclosure.

Enforcement

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

12. IT Handbook Acknowledgement

I acknowledge that I have received a copy of the SitusAMC IT Policy Handbook ("IT Handbook") and was advised to read the IT Handbook thoroughly.

I have familiarized myself with the information in the IT Handbook and will observe the policies and procedures set forth therein.

I understand that this IT Handbook supersedes and replaces all previously issued IT Handbooks and/or policies, prior to the date of this IT Handbook, unless otherwise stated in this IT Handbook.

I understand that the policies, practices, and benefits set forth in this IT Handbook are presented as a matter of information only.

I recognize that SitusAMC may, on a non-retroactive basis, modify, revoke, suspend or change any or all of such policies, practices, and benefits at any time with or without any notice, except the "at-will" nature of my employment. These policies, practices, and benefits and the IT Handbook do not modify the "at-will" nature of my employment or imply any limit on the right of SitusAMC or my right to terminate the employment relationship for any lawful reason or no reason, at any time, with or without notice, and with or without cause.

I agree to abide by all the policies, practices, and benefits as described in the IT Handbook, and all other policies, practices, and benefits established by SitusAMC that may not be in the IT Handbook, but still govern my employment.

I agree and understand that I am voluntarily waiving my constitutional right to a jury trial in connection with any dispute or claim concerning or relating to the IT Handbook or the terms and conditions of my employment with SitusAMC.

I understand that I am an "at-will" employee, and that either SitusAMC or I may terminate the employment relationship for any lawful reason or no reason. at any time. with or without prior notice, and with or without cause.

Additionally, I understand that the IT Handbook does not create any express or implied contract of any kind.

Employee's Printed Name: _____

Employee's Signature: _____

Date: _____