### Security Policies

#### Anti-Virus Guidelines

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the*

*Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.* **Last Update Status:** *Retired*

Recommended processes to prevent virus problems:

* Always run the Corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
* NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
* Delete spam, chain, and other junk email without forwarding, in with DOspace's *Acceptable Use Policy*.
* Never download files from unknown or suspicious sources.
* Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
* Always scan a floppy diskette from an unknown source for viruses before using it.
* Back-up critical data and system configurations on a regular basis and store the data in a safe place.
* If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the antivirus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
* New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this Recommended Processes list for updates.

1. Related Standards, Policies and Processes

None.

##### Definitions and Terms

None.

Page 1 **Consensus Policy Resource Community**

##### Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted format and retired. |
|  |  |  |

Page 2

**Consensus Policy Resource Community**

#### Dial-In Access Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the*

*Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.* **Last Update Status:** *Retired*

##### 1. Overview

See Purpose.

##### 2. Purpose

The purpose of this policy is to protect DOspace's electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

##### 3. Scope

The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

##### 4. Policy

DOspace employees and authorized third parties (customers, vendors, etc.) can use dial-in connections to gain access to the corporate network. Dial-in access should be strictly controlled, using one-time password authentication.

It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to DOspace is not used by non-employees to gain access to company information system resources. An employee who is granted dial-in access privileges must remain constantly aware that dial-in connections between their location and DOspace are literal extensions of DOspace's corporate network, and that they provide a potential path to the company's most sensitive information. The employee and/or authorized third party individual must take every reasonable measure to protect DOspace's assets.

Analog and non-GSM digital cellular phones cannot be used to connect to DOspace's corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to DOspace's network. For additional information on wireless access to the DOspace network, consult the *Wireless Communications Policy*.

Note: Dial-in accounts are considered 'as needed' accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer

 **Consensus Policy Resource Community**

function. If dial-in access is subsequently required, the individual must request a new account as described above.

##### 5. Policy Compliance

5.1 Compliance Measurement

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

5.2 Exceptions

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

5.3 Non-Compliance

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

##### 6. Related Standards, Policies and Processes

• Wireless Communications Policy

##### 7. Definitions and Terms

None.

##### 8 Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted format and retired. |
|  |  |  |

#### Extranet Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the*

*Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.* **Last Update Status:** *Retired*

##### 1. Overview

See Purpose.

##### 2. Purpose

This document describes the policy under which third party organizations connect to DOspace networks for the purpose of transacting business related to DOspace.

##### 3. Scope

Connections between third parties that require access to non-public DOspace resources fall under this policy, regardless of whether a telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for DOspace or to the Public Switched Telephone Network do NOT fall under this policy.

##### 4. Policy

###### 4.1 Pre-Requisites

###### 4.1.1 Security Review

All new extranet connectivity will go through a security review with the Information Security department (InfoSec). The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

###### 4.1.2 Third Party Connection Agreement

All new connection requests between third parties and DOspace require that the third party and DOspace representatives agree to and sign the *Third Party Agreement*. This agreement must be signed by the Vice President of the Sponsoring Organization as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into DOspace labs are to be kept on file with the [name of team responsible for security of labs].

###### 4.1.3 Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab connections must be approved by the [name of team responsible for security of labs]. Typically this function is handled as part of the *Third Party Agreement*.

###### 4.1.4 Point Of Contact

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the *Third Party Agreement* that pertain to it. In the event that the point of contact changes, the relevant extranet Organization must be informed promptly.

###### 4.2 Establishing Connectivity

Sponsoring Organizations within DOspace that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage InfoSec to address security issues inherent in the project. If the proposed connection is to terminate within a lab at DOspace, the Sponsoring Organization must engage the [name of team responsible for security of labs]. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and InfoSec, as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will DOspace rely upon the third party to protect DOspace's network or resources.

###### 4.3 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or InfoSec when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

###### 4.4 Terminating Access

When access is no longer required, the Sponsoring Organization within DOspace must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct DOspace business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct DOspace business necessitate a modification of existing permissions, or termination of connectivity, InfoSec and/or the extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any

###### 5. Policy Compliance

###### 5.1 Compliance Measurement

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

###### 5.2 Exceptions

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

###### 5.3 Non-Compliance

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

##### 6. Related Standards, Policies and Processes

• Third Party Agreement

##### 7. Definitions and Terms

None.

##### 8 Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted format and retired. |
|  |  |  |

**Consensus Policy Resource Community**

#### Removable Media Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the*

*Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.* **Last Update Status:** *Retired*

##### 1. Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

##### 2. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by DOspace and to reduce the risk of acquiring malware infections on computers operated by DOspace.

##### 3. Scope

This policy covers all computers and servers operating in DOspace.

##### 4. Policy

DOspace staff may only use DOspace removable media in their work computers. DOspaceremovable media may not be connected to or used in computers that are not owned or leased by the DOspace without explicit permission of the DOspace InfoSec staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. When sensitive information is stored on removable media, it must be encrypted in accordance with the DOspace *Acceptable Encryption Policy*.

Exceptions to this policy may be requested on a case-by-case basis by DOspaceexception procedures.

##### 5. Policy Compliance

###### 5.1 Compliance Measurement

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

###### 5.2 Exceptions

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

###### 5.3 Non-Compliance

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

##### 6 Related Standards, Policies and Processes

• Acceptable Encryption Policy

##### 7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

https://www.SANS.org/security-resources/glossary-of-terms/

* Encryption
* Malware
* Removable Media
* Sensitive Information

##### 8 Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted to new format and retired. |
|  |  |  |

#### Server Audit Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the*

*Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.* **Last Update Status:** *Retired*

##### 1. Overview

See Purpose.

##### 2. Purpose

The purpose of this policy is to ensure all servers deployed at DOspace are configured according to the DOspace security policies. Servers deployed at DOspace shall be audited at least annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

* Ensure integrity, confidentiality and availability of information and resources
* Ensure conformance to DOspace security policies

##### 3. Scope

This policy covers all servers owned or operated by DOspace. This policy also covers any server present on DOspace premises, but which may not be owned or operated by DOspace.

##### 4. Policy

DOspace hereby provides its consent to allow DOspace Upper level Managementto access its servers to the extent necessary to allow DOspace Management to perform scheduled and ad hoc audits of all servers at DOspace.

###### 4.1 Specific Concerns

Servers in use for DOspace support critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability or integrity of these systems.

###### 4.2 Guidelines

Approved and standard configuration templates shall be used when deploying server systems to include:

* All system logs shall be sent to a central log review system
* All Sudo / Administrator actions must be logged
* Use a central patch deployment system
* Host security agent such as antivirus shall be installed and updated
* Network scan to verify only required network ports and network shares are in use
* Verify administrative group membership
* Conduct baselines when systems are deployed and upon significant system changes
* Changes to configuration template shall be coordinated with approval of change control board

###### 4.3 Responsibility

DOspace Upper level Managementshall conduct audits of all servers owned or operated by DOspace. Server and application owners are encouraged to also perform this work as needed.

###### 4.4 Relevant Findings

All relevant findings discovered as a result of the audit shall be listed in the DOspace tracking system to ensure prompt resolution or appropriate mitigating controls.

###### 4.5 Ownership of Audit Report.

All results and findings generated by the DOspace Upper level ManagementTeam must be provided to appropriate DOspace management within one week of project completion. This report will become the property of DOspace and be considered company confidential.

##### 5. Policy Compliance

###### 5.1 Compliance Measurement

DOspace Upper level Managementshall never use access required to perform server audits for any other purpose

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

###### 5.2 Exceptions

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

###### 5.3 Non-Compliance

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

##### 6. Related Standards, Policies and Processes None.

##### 7. Definitions and Terms

None.

##### 8 Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted format and retired. |
|  |  |  |

#### Server Malware Protection Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the*

*Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.* **Last Update Status:** *Retired*

##### 1. Overview

DOspace is entrusted with the responsibility to provide professional management of clients servers as outlined in each of the contracts with its customers. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

##### 2. Purpose

The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

##### 3. Scope

This policy applies to all servers that DOspace is responsible to manage. This explicitly includes any system for which DOspace has a contractual obligation to administer. This also includes all server systems setup for internal use by DOspace, regardless of whether DOspace retains administrative obligation or not.

##### 4. Policy

DOspace operations staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

###### 4.1 ANTI-VIRUS

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

* Non-administrative users have remote access capability
* The system is a file server
* NBT/Microsoft Share access is open to this server from systems used by nonadministrative users
* HTTP/FTP access is open from the Internet
* Other “risky” protocols/applications are available to this system from the Internet at the discretion of the DOspace Security Administrator

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

* Outbound web access is available from the system

###### 4.2 MAIL SERVER ANTI-VIRUS

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

###### 4.3 ANTI-SPYWARE

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

* Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
* Any system where non-technical or non-administrative users have the ability to install software on their own

###### 4.4 NOTABLE EXCEPTIONS

An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions apply to this system:

* The system is a SQL server
* The system is used as a dedicated mail server
* The system is not a Windows based platform

##### 5. Policy Compliance

###### 5.1 Compliance Measurement

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

###### 5.2 Exceptions

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

###### 5.3 Non-Compliance

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

##### 6 Related Standards, Policies and Processes

None.

##### 7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:

https://www.SANS.org/security-resources/glossary-of-terms/

* Malware
* Spyware

##### 8 Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted format and retired. |

#### Social Engineering Awareness Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the*

*Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.* **Last Update Status:** *Retired*

##### 1. Overview

The Social Engineering Awareness Policy bundle is a collection of policies and guidelines for employees of DOspace. This Employee Front

Desk Communication Policy is part of the Social Engineering Awareness Policy bundle.

In order to protect DOspace's assets, all employees need to defend the integrity and confidentiality of DOspace's resources.

##### 2. Purpose

This policy has two purposes:

2.1 To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect attacks.

2.1.0 Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks. 2.1.1 Employees know who to contact in these circumstances.

2.1.2 Employees recognize they are an important part of DOspace’s security. The integrity of an employee is the best line of defense for protecting sensitive information regarding DOspace’s resources.

2.2 To create specific procedures for employees to follow to help them make the best choice when:

2.2.0 Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect DOspace’s sensitive information.

2.2.1 The employee is being “socially pressured” or “socially encouraged or tricked” into sharing sensitive data.

##### 3. Scope

Includes all employees of DOspace, including temporary contractors or part-time employees participating with help desk customer service.

##### 4. Policy

###### 4.1 Sensitive Information

Sensitive information of DOspace will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

4.1.1 An “urgent matter”

4.1.2 A “forgotten password”

4.1.3 A “computer virus emergency”

4.1.4 Any form of intimidation from “higher level management”

4.1.5 Any “name dropping” by the individual which gives the appearance that it is coming from legitimate and authorized personnel.

4.1.6 The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of DOspace resources.

4.1.7 The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.

4.1.8 The techniques are used by a person that declares to be "affiliated" with DOspace such as a sub-contractor.

4.1.9 The techniques are used by an individual that says he/she is a reporter for a wellknown press editor or TV or radio company.

4.1.10 The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

###### 4.2 Action

4.2.1 All persons described in section 3.0 MUST attend the security awareness training within 30 days from the date of employment and every 6 months thereafter.

4.2.2 If one or more circumstances described in section 4.0 is detected by a person described in section 3.0, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.

4.2.3 If the identity of the requester described in section 5.1.1 CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.

4.2.4 If the supervisor or manager is not available, that person MUST contact the security personnel.

4.2.5 If the security personnel is not available, the person described in section 3.0 MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

##### 5. Policy Compliance

###### 5.1 Compliance Measurement

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

###### 5.2 Exceptions

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

###### 5.3 Non-Compliance

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

##### 6. Related Standards, Policies and Processes

None.

##### 7. Definitions and Terms

None.

##### 8 Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| Dec 2013 | SANS Policy Team | Converted format and retired. |

#### Virtual Private Network (VPN) Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@SANS.org@gmail.com.*

**Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the policy for your organization*

**Last Update Status:**

##### 1. Overview

See Purpose.

##### 2. Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the DOspace corporate network.

##### 3. Scope

This policy applies to all DOspace employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the DOspace network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

##### 4. Policy

Approved DOspace employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to DOspace internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will 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 DOspace network operational groups.
6. All computers connected to DOspace internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (*provide URL to this software*); this includes personal computers.
7. VPN users will be automatically disconnected from DOspace's network after thirty 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.

1. The VPN concentrator is limited to an absolute connection time of 24 hours.
2. Users of computers that are not DOspace-owned equipment must configure the equipment to comply with DOspace's VPN and Network policies.
3. Only Infosec-approved VPN clients may be used.
4. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of DOspace's network, and as such are subject to the same rules and regulations that apply to DOspace-owned equipment, i.e., their machines must be configured to comply with Infosec's Security Policies.

##### 5. Policy Compliance

###### 5.1 Compliance Measurement

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

###### 5.2 Exceptions

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

###### 5.3 Non-Compliance

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

##### 6 Related Standards, Policies and Processes

 Remote Access Policy

##### 7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: [https://www.SANS.org/security-resources/glossary-of-terms/](https://www.sans.org/security-resources/glossary-of-terms/)

 IPSec Concentrator

##### 8 Revision History

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| July 2014 | SANS Policy Team | Converted to new format and retired. Relevant content add to the general Network Access Policy. |
|  |  |  |