Network Security

Table of Contents

Getting Started

In order to secure the information that flows across internal networks and to/from the Internet, colleges and universities need to effectively manage their physical and logical network infrastructure. The protection of networked information assets requires policies, standards, and a sound network control strategy. If you are just getting started in this area of your security program, then the following steps can be very helpful to get underway:

1. **Develop** policies and standards that support the:
    a. Establishment of clear authority and accountability for network management.
    b. Risk based segregation of groups of systems, users, and information systems
    c. Authority to control, actively monitor, and log traffic traversing designated ingress and egress points.
2. **Identify** threats related to the communications environment. (see HEISC Risk Management Framework)
    a. Evaluate threat scenarios and methods of network attack (reconnaissance, exploitation, data exfiltration)
3. **Identify** the most critical systems, data, or equipment within the network. (see Asset Management)
4. **Use** routing and firewalls to define the network perimeter.
5. **Use** a border firewall and/or Intrusion Detection/Prevention devices to limit entry/exit of network traffic.
6. **Define** the “demilitarized zone” of the network where the public can access limited network resources, as well as public access points to the network such as open access ports and public WiFi.
7. **Define** restricted portions of the network for use by authorized staff and facility personnel; use identity and access management controls for users and systems on the network.
8. **Define** highly restricted portions of the network such as within data centers, communications facilities, or other highly restricted areas.
9. **Establish** information transfer policies and encryption standards that address varied needs for confidentiality, integrity, and non-repudiation of internal and external data exchanges.

Top of page

Overview

Communications encompasses the breadth of digital data flows both within an organization and between external entities across network infrastructures. These flows now include data, voice, video, and all of their associated signaling protocols. Securing these information flows as they traverse Intranets, Extranets, and Internet requires effective network infrastructure management as well as controls, policies, and procedures. This chapter provides guidance in planning, developing, and implementing the most essential elements of a Communications Security strategy.

Top of page

Network Security Management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

Establishing Responsibility and Procedures for Network Management and Operations

Information flowing across networks cannot be secured without effective management of the physical and logical network infrastructure, including physical cabling, logical topologies, network devices, and network services. A centralized entity with appropriate responsibility and authority is generally the most effective way to ensure consistency and manageability across the University's Intranet and Extranets. In many universities, achieving a single point of responsibility and authority for all network infrastructure can be challenging. Management of network infrastructure includes network operations, which is a separate function from data center or information processing operations. Network security operations is often another distinct function, but must coordinate closely with network operations.

Network controls

Overview

The large scale and high complexity of modern networks in Higher Education contributes to a challenging environment for security professionals and network administrators. The fundamental aspects of network services and protocols were not designed with information confidentiality in mind. Network Controls have been designed and implemented to compensate for this lack of security and continue to evolve as threat actors and their attack methods become more sophisticated.

Methods of Attack

Before determining which controls should be implemented and in which order, it is helpful to understand the common methods of attack. Note that a risk management approach is recommended to fully analyze all threats and responses. See the section Risk Management in this guide for more information.

The ultimate goal of attackers is to gain access to or modify data of value. Their targets are typically servers, workstations, or other computers connected to your University's networks, but they will make use of networks, other computers, people, or any other tool to achieve their objectives. Their attack strategies typically involve some form of reconnaissance, followed by exploitation – attempts to bypass or disable network or host security controls by exploiting vulnerabilities, and finally data modification or exfiltration. A Denial of Service (DoS) is a specific type of attack designed to disrupt operations or make networks and systems unavailable.

Reconnaissance – Attackers use reconnaissance to discover networks, hosts, or vulnerabilities. A variety of freely available tools are available that allow scanning or probing of systems accessible to the Internet. In targeting a specific University, an attacker need only know publicly available information such as the range of IP subnets used by the school. Scanning often involves discovering what TCP or UDP ports are active on the various hosts within the University's networks. Firewalls, IDS/IPS, network isolation, authentication, and logging are some of the tools network or security administrators use to limit or detect reconnaissance activities.

Exploitation – The protocols used across the Internet and within University Intranets and Extranets were designed for availability and openness rather than security and privacy. Attackers abuse and exploit the inherent lack of security of TCP/IP and the other various protocols and their associated network devices to their advantage. Their specific methods are numerous and varied, but can generally be categorized as follows:

- Sniffing – intercepting and examining network traffic
- Spoofing – impersonating a network host or user
- Man-in-the-Middle – covertly impersonating an intermediary host or network service such that the parties on either end of the connection are unaware that their communications are being captured and possibly altered
- Hijacking – taking over or re-routing one end of an otherwise valid communication between two parties
- Replay attacks – using intercepted communications or authentication interactions to falsely authenticate
- Password Cracking – using sophisticated or simple brute force attacks to guess weak passwords
- System or Application exploitation – once an attacker is in contact with a system at any of the application layer protocols such as FTP, Telnet, SSH, HTTP, HTTPS, SNMP, and others, weaknesses in the Operating System or the applications can be exploited to gain unauthorized access

Data Modification and Exfiltration – Once access to systems or data is gained, the data can be modified or copied (exfiltrated). While data owners might quickly know if data is modified, data exfiltration can take place in relative secrecy unless there are sufficient monitoring and controls in place to detect it. Most Universities have reasonable protections in place to prevent or detect external attacks, but are not as diligent in monitoring outbound traffic to detect confidential or sensitive data that is being copied by a successful attacker.

Control Types

Like other types of security controls, network controls can be categorized into various types, depending on their primary function.

Preventive controls seek to stop or prevent attacks or intrusions **before** they occur. Firewalls, Intrusion Prevention Systems, Web Gateways, and physical Isolation of network cabling and devices are all examples of preventive controls.

Detective Controls seek to detect attacks or intrusions in progress or after (ideally very soon after!) they have already taken place. Intrusion Detection Systems, Log collection and review, Security Information and Event Management (SIEM) systems, AntiVirus software, and video surveillance in data centers and communications facilities are examples of detective controls.

Administrative controls direct users – employees, faculty, students, contractors, and partners – to follow specific procedures. Examples include policies against connecting rogue hubs, switches, or routers to the network, the use of network traffic sniffers, unauthorized network services, and procedures for provisioning network access accounts.

Technical controls often enforce administrative controls, but can also limit or prevent network activity/traffic, or isolate network segments or users to increase overall security. Examples include network access control, group policy objects, strong authentication, encryption, and Virtual Private Network (VPN) technology.

Defense In-Depth

A sound network control strategy employs the concept of Defense In-Depth to provide optimal security. Firewalls at the network perimeter limit the traffic that is allowed in and out of the network. IDS/IPS devices detect and prevent traffic that is suspicious or known to be malicious. Internal network isolation limits the visibility of network traffic to devices and users by department or role. Access to wireless and wired networks are restricted to authenticated University faculty, staff, and students only. Strong passwords are enforced for all network computers. Computers run host-based firewalls and AntiVirus software. Certain sensitive network traffic is encrypted so that it cannot be intercepted. All of these controls are combined together to provide a layered or In-Depth defensive strategy.

Network Design and Architecture

Centralized management of University networks allows for a strategic network design and architecture that can be more readily optimized for performance, availability, and security. All endpoints should terminate to network switches to remove the possibility of internal network traffic sniffing by computers and users. Highly sensitive data and traffic such as for Data Centers or communications facilities should be isolated through virtual LAN (vLAN) technology and /or Firewalls. Highly unregulated traffic such as for student residence halls should also be isolated. For more information, see section 13.2 Network Isolation.

The architecture of the network should allow for the strategic placement of firewalls, demilitarized zones (DMZ's), and IDS/IPS devices such that all network traffic between the University Intranet and the Internet can be adequately controlled and monitored.

Perimeter Controls

Perimeter controls must be strategically placed such that all network traffic flowing in and out of the University's internal networks, i.e. its Intranet, can be controlled and monitored. These controls are critical to network functionality and security and therefore must be fault-tolerant and have redundant backups available. In addition, they must be capable of processing the anticipated peak volume of network traffic. This is especially important for larger Universities with extremely high aggregate Internet bandwidth. Typical perimeter controls include:

- Routers – The border router is typically capable of allowing or denying connections, but it's primary purpose is to route traffic at the network border or DMZ
- Firewalls – firewalls (sometimes called border firewalls) block or limit traffic, typically by TCP/UDP port
- IDS/IPS – An Intrusion Detection System and/or Intrusion Prevention System adds an extra layer of protection, examining, limiting, or blocking traffic that was allowed through the border firewall, but is highly suspicious or known to be malicious
- Data Loss Prevention (DLP) – some DLP solutions inspect all network traffic to detect or block confidential data from leaving the Intranet
- "Next Generation" Firewalls – The term "NextGen" is a marketing term used by some vendors to imply a higher level of sophistication and thus a higher level of protection. While many of these products do perform as advertised, they are essentially serving the same or combined functions as firewall and IDS/IPS technology.
- Web Gateway – A *secure* web gateway does not necessarily sit at the perimeter, but does filter web-based traffic, providing more granular IDS /IPS functionality for web-based traffic or content
- Network Address Translation (NAT) – not strictly a security control, NAT limits the visibility of endpoints within the University Intranet from potential attackers on the Internet.

Note on encryption – while encryption is an effective control for data in transit, security administrators should also be aware that too much encryption of network traffic can severely limit many perimeter controls such as IDS/IPS, DLP, and Secure Web Gateways.

Many vendors are now providing cloud-based network protection, which can supplement or replace many of the on-premise perimeter or interior controls network and security administrators have used.

Interior/Endpoint Controls

Isolation - Network segments or subnets within the University Intranet should be appropriately isolated according to the security requirements of the users and endpoints. Virtual LAN (vLAN) technology is the primary control used to isolate users and endpoints. Some typical segments might include Residence Halls, Research, PCIDSS, Data Center, Surveillance, Alarm Systems, and WiFi. See section 13.1.3 for more information on network isolation.

Endpoint Hardening - All network devices and endpoints should be hardened to reduce their attack surface. Hardening involves maintaining current patch levels, AntiVirus, host-based firewalls, host-based IDS/IPS, disabling unnecessary services, using strong passwords, and other protections as appropriate. Software whitelisting can also provide additional endpoint protection. Network and security administrators should not neglect printers, multi-function devices, and other network-attached devices which often have unsecure services opened up, such as FTP, Telnet, or SNMP.

Vulnerability Management - A Vulnerability Management System can help ensure that all endpoints on the network are adequately hardened. Vulnerability Management should ideally include web-based applications to reduce vulnerability to SQL-Injection, Cross-Site Scripting, and other web-based exploits.

Network Access Control (NAC) – Registering all endpoints before allowing connection to the network can prevent unauthorized devices from connecting as well as enforce security baselines. For instance, University IT Security Policies may state that all endpoints have automatic security updating enabled, authentication must be done via the central Active Directory domain, and AntiVirus and Firewall must be active. NAC can prevent systems which do not meet these requirements from accessing all or certain portions of the network.

WiFi Security Controls – Campus WiFi should be protected and in most cases, isolated from all other internal networks, particularly when the University has chosen to make WiFi open-access. Open-access WiFi allows any computer within range to connect and therefore should be provided limited services such as Internet access only. WiFi that connects to more sensitive portions of the network should be limited to authorized users only. All WiFi should use WPA2 or stronger encryption. Note that enabling these levels of control across a large campus can be costly and require sophisticated equipment.

Remote Access – remote access to internal or Intranet networks can be a high security risk if not properly planned and secured. While a Virtual Private Network (VPN) service is an excellent way to allow remote users to securely connect to your internal networks or Intranet, it provides no assurance that the connecting endpoint computer is itself secure. Security administrators should strongly consider enforcing Network Access Control for VPN connections or strictly limiting the use of VPN to selected trusted users. Outbound VPN can also introduce risk of opening up internal networks to potentially unsecure external networks. Many Universities chose to block outbound VPN at the firewall for this reason.

Other remote access tools and protocols need to be carefully controlled or limited. Remote Desktop Protocol (RDP) and Secure Shell (SSH) can introduce additional risk. RDP is best blocked at the firewall or provided through an RDP Gateway. While SSH is a secure protocol, the Linux and Unix systems that typically use SSH are often administered outside of the campus directory service and can thus have weak passwords. External attackers routinely look for open SSH ports and attempt to use Rainbow tables or Brute Force to crack passwords.

Web-based services such as LogMeIn, VNC, GoToMyPC, etc. can also introduce risk of unauthorized remote access. Security administrators should carefully assess the risks associated with these services.

Back Doors – Remote Access protocols and services can create "back doors" of access into internal networks and should be carefully administered. Other back doors include analog modems, cellular services on smartphones and tablets, Bluetooth personal area networks, and removable media such as USB and CD/CDRW drives.

Encryption

Encryption of certain network traffic is an essential network control. All confidential or sensitive information leaving the network should be encrypted with proven strong encryption algorithms. Authentication protocols that transmit passwords or encryption keys over the network should also be encrypted. Secure Sockets Layer (SSL) is a common encryption protocol used for web traffic.

Network Security Policies

A strong set of network security policies complements technical controls. While policies cannot always be technically enforced, users need to be aware of behaviors that are unacceptable by policy. Examples include:

- Use of strong passwords
- No sharing of user account credentials
- Users are not allowed to install and run illegal software, such as network sniffing/scanning or P2P File Sharing software
- All user accounts must be centrally managed and issued
- Prohibition of rogue switches, routers, hubs

- All network cabling and outlets must be installed by central network services
- Limited expectation of privacy

Security policies provide a means of enforcement in the event of known violations.

Log Management and Auditing

Routers, switches, IDS/IPS, firewalls, Directory Services controllers, and other network devices have a wealth of information about activity on the network. However, the massive amount of data they produce makes it difficult to adequately correlate and review for possible intrusions or perform forensic investigations. A Security Information and Event Management (SIEM) solution can greatly reduce the effort and expense involved and provide a much higher level of visibility for security. Network Access Control

Penetration Testing

All network controls should be routinely validated by an authorized external third party. The process is typically referred to as Penetration Testing (Pen Tests). A qualified Pen Tester can help ensure that the controls you have carefully implemented are working effectively. Many Universities are required to perform such testing on an annual or biennial basis.

Security of network services

Overview

Network services include Directory services, Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), authentication services, messaging/email, remote access, and others. These services have traditionally been provided on premise by network and/or security administrators. Today, many Universities are turning to outsourced cloud providers for many of these services.

On Premise Services

Most campuses utilize some form of Directory Service, such as Microsoft Active Directory. Other essential services include DHCP, DNS, and remote access service such as VPN. Because these services operate at the network and IP layers of the OSI stack, and they perform essential functionality for all network hosts, they must be well-managed and secured. Only a very small number of network administrators should have administrative access to the underlying servers. These servers must also be hardened and kept up to date with security patches. Logging to an external aggregator or SIEM is also strongly recommended.

External Network Services

Highly available Internet connectivity has opened the door for Universities and other organizations to shift network and other application services to external cloud providers. While there are many reputable and very capable providers, it is nonetheless more difficult to hold an external entity accountable at the same levels possible with internal staff. Universities entering into agreements with cloud providers need to carefully review and negotiate the specific terms and conditions of these agreements. Service Level Agreements, Confidentiality Statements, and Privacy Policies are among the types of documents that must be carefully reviewed and updated. The default versions of these documents will typically be written in favor of the external provider rather than their customers. External service providers should be held to the same level of security controls as those that apply to internal services. Universities should write into their agreements language that specifies required security controls, limitation of access by provider's employees, confidentiality statements, the right of the University to audit security controls, and any other provisions that reduce risks of data disclosure, alteration, or loss.

Segregation in networks

One way to protect your confidential and/or critical systems is to segregate your networks along physical or logical lines. Using VLANs to separate your systems creates an additional layer of security between your regular network and your most sensitive systems. This method is often utilized in order to protect data centers, credit card processing systems covered by PCI DSS, SCADA systems, and other systems considered to be sensitive or mission critical.

In order to properly control access to your segregated networks, you should place a firewall or router at the perimeter of each network. That way, different networks can have different access control policies based on the sensitivity classification of the data that they create, transmit, and/or store. Special consideration should be given to wireless networks that allow anyone to connect for Internet access – if you offer an unsecured connection to your wireless network, you should take steps to ensure that wireless traffic is kept separate from the rest of your network or networks. Wireless users should not be able to access domain resources on your wired network without authenticating first, at least; most organizations now offer a secure wireless option (sometimes in addition to a separate, cordoned-off unsecure wireless option) to help maintain the confidentiality and integrity of their wired network.

- UNC-G: Wireless Networking
- Appalachian State University: Open Servers VLAN Policy

Top of page

Information Transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

Information transfer policies and procedures

Clear policies and procedures that govern the transfer of information between individuals both within and outside your organization should be established. Be sure to consider all possible methods of communication, including face-to-face, e-mail, voice, fax, and video, when drafting your policies.

General policies about information transfer should include guidelines for acceptable use, and more specific procedures can be established to ensure secure transfer using approved methods. Make sure your users are aware of the limitations of each system (e.g., transferring information via fax machine is only a secure option if physical access to the machine on the other end is restricted).

In addition to establishing policies, technical controls should be implemented, when feasible, to protect the confidentiality, integrity, and availability of the information being transferred. Most anti-virus and anti-malware solutions have tools that can scan e-mails in real time, and encrypting important e-mails can be done for free (using PGP, for instance) or implemented enterprise-wide. These controls can provide a first line of defense against infection and/or compromise. It is still important, however, to discuss information transfer as a part of your organization's information security awareness program. Educating your users about not communicating confidential information over insecure channels, state and organizational retention guidelines, and the dangers of e-mail auto-forwarding, among other topics, can go a long way toward ensuring that your systems and data remain secure.

- University of Missouri: Systems Electronic Records Administration
- University of Miami School of Medicine: Privacy/Data Protection Project

Top of page

Agreements on information transfer

If your organization has a business need to transfer information to a third party, then you should (and, in some cases, are legally required) to enter into an official agreement with them in order to preserve the security of that information. These agreements generally set minimum standards for protecting your data, and may also establish the limits of liability for both parties in the event of a breach or other unauthorized disclosure of data.

If the data being transferred is considered HIPAA-protected (under the Health Insurance Portability and Accountability Act of 1996), then the two parties must enter into a Business Associate Agreement (BAA). BAA's are required to include clauses covering data security (pursuant to the HIPAA Security Rule), data disclosure, and data destruction, among others. Similarly, if the data is not HIPAA-protected but is still considered highly sensitive (e.g., social security numbers, bank account numbers), then your organization may require additional data security provisions, similar to those found in a BAA, for such a contract.

Information transfer agreements may also include the following: agreed upon cryptographic standards for encrypting data in transit and at rest, and chain of custody for physical transfer. For example, any agreement between your organization and a company that provides off-site backup storage for your critical systems and data should include clauses that cover minimum standards for protection of your data in transit from one location to the other (e.g., are the tapes secured in a locked box? Who has the key?), and procedures for identifying and authorizing individuals from one organization or the other (since neither company can reasonably be expected to know all the other's employees).

- HHR: Sample Business Associate Agreement Provisions
- HHR: HIPAA Security Rule Guidance Material

Top of page

Electronic messaging

Electronic messaging includes e-mail, peer-to-peer file transfer, social network-based communications (e.g., Google Hangouts, Facebook chats, LinkedIn InMail, etc.) and more. Your organization should consider introducing a policy that governs the authorized use of these mediums; at a minimum, such a policy should establish the authority to represent your organization in an official capacity on the Internet. Also, because your organization is unable to apply technical controls to third-party electronic messaging mediums – Google Hangouts, Facebook, et. al. – there is no way for you to quantify or improve their level of security in order to effectively secure a confidential message traveling across one of these mediums. The solution to this problem is to clearly state in your policy that organization-related business is only to be communicated and/or conducted using approved, secured methods (e.g., e-mail).

- Tennessee Board of Regents: Use of Electronic Signatures & Records
- Drexel University: Social Media Policy

Top of page

Confidentiality or non-disclosure agreements

Confidentiality or non-disclosure agreements are legally enforceable documents designed to protect your organization's confidential information and intellectual property. These agreements, signed by the organization and its employees and/or third parties, establish the responsibilities of all parties to ensure that no one discloses sensitive data in an unauthorized manner.

- UM Research and Sponsored Projects: Disclosure and Confidentiality Agreements
- KU: Confidentiality Agreement Requests

Top of page

Resources

EDUCAUSE Resources

EDUCAUSE Resources & Resource Center Pages

- Communications
- Usability and Network Security in Higher Education
- Network Security
- PCI DSS (Payment Card Industry Data Security Standard)
- Security Management
- 7 Things You Should Know About Cloud Security
- Cloud Computing Security
- Dropbox Security & Privacy Considerations

HEISC Toolkits/Guidelines

- E-Discovery Toolkit
- Electronic Records Management Toolkit
- Guidelines for Data De-Identification or Anonymization
- Guidelines for Information Media Sanitization
- Two-Factor Authentication

Templates/Sample Plans

- University of Houston Information Security Resources and Operations Manual
- Indiana University Data Center
- Northwestern University Information Technology Information and Systems Security/Compliance
- University of Missouri Systems Records Management General Policy

Security Professionals Conference 2014

- HTML5 Security

Security Professionals Conference 2013

- Bring Your Own Cloud: Data Management Challenges in a Click-Through World

Enterprise IT Leadership Conference 2013

- Providing Private Cloud Services To Support HIPAA Compliance

EDUCAUSE Annual Conference 2012

- Reaching a Higher Elevation: Supporting High-Value, High-Risk Cloud Services
- Raising the Bar in Cloud Security for Higher Education
- Community and the Cloud: Shaping the Future of Technology Services for Higher Education

Security Professionals Conference 2012

- Tools and Methods for Managing SNORT Sensors in Distributed Environments
- DNS Sinkholing to Reduce Network Compromises

Southeast Regional Conference 2012

- The EITS Analysis Committee: A Grassroots Effort at Standardized Documentation and Diagramming Templates
- Personal Storage in the Cloud

Mid-Atlantic Regional Conference 2012

- Leverage the Cloud + Leverage In-House + Improve Security = Save Money

EDUCAUSE Annual Conference 2011

- Building a Business Case for the Cloud
- The Titan Cloud: CSU Fullerton's Virtual Computing Infrastructure Implementation

Security Professionals Conference 2011

- Information Technology Standards at the University of Illinois: Common Challenges and Solutions
- Network Segmentation: Virtual Routing Implementation
- Seminar 02P - Malware Detection and Mitigation with Passive DNS and Blackhole DNS
- A Gentle Introduction to Bro
- Do They Measure Up? Assessing the Security Posture of Third-Party Service Providers

EDUCAUSE Annual Conference 2010

- Cloud Computing Security: An Oxymoron?
- Deploying an Internal Cloud: Offering Infrastructure as a Service to the Campus Community
- Building a Network Control Strategy for Your Campus
- Cloud Computing Contract Issues
- Steps to a Cloud-Ready Data Center
- Shared Data Centers: Something Old and Something New

Security Professionals Conference Archives 2008-2010

Management and Operations:

- Building a Cybersecurity Operations Center
- A Normative Campus Security Agenda

Corporate and Campus Solutions:

- How to Use NetFlow to Gain Internal Visibility and Security
- Realizing the Promise of Faster, More Secure Campus Communications
- Symantec Corporation and Temple University - Securing a Free and Open University Environment
- McAfee and Georgia State University - Taking Aim at Network Intruders with Intrushield's Intrusion Prevention System
- FireEye, Inc. and University of California, Berkeley - Combating Stealth Malware and Botnets in Higher Education

Technology Concepts:

- Filelocker: Simplifying Secure File Transfers
- Web Application Firewalls at SCSU: Why and How
- Virtualization and Security Architecture
- Securing and Leveraging the Power of Virtual Servers and Desktops

Advanced Technology:

- Mastering Puppet: Using Puppet to Centrally Manage IT Security Infrastructure
- Starting Over from the Top: Campus IPv6 Deployment and Security
- Linking Remote Sites with OpenVPN
- Network Monitoring with Argus, NetFlow, and Other Tools
- Improving Security Event Correlation and Analysis Using Intelligent Agents
- REN-ISAC and CSI2---The Security Event System

Initiatives, Collaborations, & Other Resources

- ECAR Working Groups; Bring together higher education IT leaders to address core technology challenges.

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management **Chapter 13**: Communications Security **ISO/IEC 18028-4:2005** **ISO/IEC 27033-1:2009**	**800-100**: Information Security Handbook: A Guide for Managers **800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems	**APO01.06** **APO13.01** **DSS05.02** **DSS06.06**	**Req 6** **Req 12**	**ID.AM-3** **PR.AC-3** **PR.AC-5** **PR.DS-2** **PR.DS-5** **PR.PT-4**	**45 CFR 164.314 (a)(1)** **45 CFR 164.308 (b)(4)** **45 CFR 164.314 (a)(2)(i)** **45 CFR 164.314 (a)(2)(ii)** **45 CFR 164.312 (e)(1)**

Top of page

Questions or comments? Contact us.