Virginia Tech IT Security Office
Implementing The 20 Critical Security Controls

www.security.vt.edu

January 9th, 2016

Contents

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to describe methods and define responsibilities for implementing the 20 Critical Security Controls at Virginia Tech. The overall goal of the controls is to ensure the confidentiality, integrity, and availability of Virginia Tech's networks, systems, and data in accordance with University Policy 7010, Policy for Securing Technology Resources and Services.

1.2 Notice

It is the reader's responsibility to ensure that they have the latest version of this document. Revision questions should be directed to the University's Information Security Officer. The most recent, approved version of this document is available on the IT Security Office's website and upon request by emailing itso@vt.edu.

Virginia Tech has standardized on Version 5.1 of the 20 Critical Security Controls.

1.3 Revision History

January 9th, 2016 - Original Version

1.4 Review Process

Virginia Tech Internal Audit and The IT Council will provide the initial review of this document and all subsequent revisions.

1.5 Approval Authority

The University IT Security Officer has approval authority over this document.

1.6 How to Implement the Controls

The controls may be implemented through policies, procedures and technical measures. The IT Security Office strongly encourages the use of technical measures whenever possible, however, we realize that technical measures are not suitable for every department and every situation.

Departments may decide to use a combination of policies, procedures and technical measures when implementing the controls. For example, Control 5 (Malware Defense) is already listed in University Policy 7010 and has a defined procedure, *"Install antivirus software and ensure virus definitions are updated regularly"*. In this case, departments may decide to use BigFix or some other endpoint management system as a technical measure to ensure that the control is indeed implemented on department systems.

1.7 How to Measure Implementation Progress

In the companion spreadsheet, each control has a metric question that corresponds with each method listed for the control. Most of these questions should be answered 'Yes' or 'No', however, some of the questions may not apply to your area. If the department answers 'Yes' or 'N/A' to all of the metric questions and can provide quantities, dates and explanations, then that control has been fully implemented.

Some methods are conditional and may not apply to all departments. When measuring the metrics for methods that do not apply to your area, please answer 'N/A' and attach a note to the spreadsheet with a brief explanation.

1.8 Implementation Responsibility

Each security control must have at least one department responsible for implementing the control. Some controls have a shared responsibility. For example, Control 7 (Wireless Access Control) should be implemented by Network Infrastructure and Services and University departments that run their own Wireless Access Points. Control 18 (Incident Response and Management) should be implemented by the IT Security Office, University management and University departments. Each security control lists the responsible parties.

1.9 Format

The security controls are described in the following format:

- Number and name of the control.
- Areas responsible for implementing the control.

- Methods for implementing the control.
- Metrics for measuring the implementation.
- Notes about implementing the security control at Virginia Tech.

2 CONTROLS

2.1 Inventory of Authorized and Unauthorized Devices

- Responsibility - University departments and Fixed Assets
- Methods
  1. Departments should create local, department policies that clearly define what authorized and unauthorized devices are in their respective areas.
  2. Departments should work with Fixed Assets inventory reports and auditors to inventory devices.
  3. Departments should occasionally spot check devices to ensure that they are authorized.
  4. Departments should use BigFix to track and inventory departmental devices.
- Metrics
  1. Has the department written a local policy that defines authorized devices?
  2. Has the department reconciled its fixed asset inventory during the last calendar year?
  3. Did the department conduct a spot check for unauthorized devices during the last six months?
  4. Does the department use BigFix or some other automated system to track departmental devices?
- Notes - When referring to computing devices, the University does not define the terms 'Authorized Devices' or 'Unauthorized Devices'. The decision as to whether or not a computing device is authorized or unauthorized for use at Virginia Tech is left to departments and area supervisors. Currently, many University employees use personal computing devices while at work. This includes personal laptops, tablets and cell phones. Departments may decide that all devices both personal and University owned are authorized for use, however, accurate, updated fixed asset inventory lists must always be maintained. Spot checks should be the responsibility of supervisors and area managers who have a good grasp on local conditions and can easily identify unauthorized devices.

2.2 Inventory of Authorized and Unauthorized Software

- Responsibility - University departments and the Information Technology Acquisitions
- Methods
  1. Departments should work with the Information Technology Acquisitions and the VT Software Distribution Office to create local, department policies that clearly define the terms 'Authorized Software' and 'Unauthorized Software' for departmental employees.
  2. Departments should install endpoint management software, such as BigFix, to inventory software installed on departmental machines and take action when unauthorized software is discovered.
  3. Departments should periodically spot check department computers for unauthorized software.
- Metrics
  1. Has the department written a local policy that defines authorized and unauthorized software?
  2. Does the department use BigFix or some other automated system to inventory installed software?
  3. Did the department perform a spot check for unauthorized software during the last six months?
- Notes - VT is very diverse and has many unique needs. The decision as to whether or not specific software is authorized or unauthorized for use is left to departments and area supervisors. So long as the software is legally purchased (or obtained) through the VT Software Distribution Office and is intended for some University purpose, then the IT Security Office would not object to its use. Obviously, the use of unlicensed or stolen software would be illegal and thus unauthorized for use at the University. It is also a violation of University Policy 7000, Acceptable Use and Administration of Computer and Communication Systems.

2.3 Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

- Responsibility - University departments and the IT Security Office
- Methods
  1. Departments should run security configuration assessment tools on departmental computing devices at least once a year and use the resulting reports to further secure the systems.
  2. Departments should restrict logical administrative access to key departmental employees who have been trained to administer systems.
  3. Departments should install and monitor file integrity checking software on all critical systems.
  4. Departments should use centralized endpoint management software, such as BigFix, Group Policy, and Ansible to ensure that departmental computing devices are securely and consistently configured.
  5. Departments should apply critical security patches as soon as practical or within 90 days of release.
- Metrics
  1. Did the department run a security configuration assessment tool during the last year?
  2. Does the department restrict administrative access to key employees who have received the appropriate level of IT administration training?
  3. Does the department use and monitor file integrity checking software?
  4. Does the department use centralized endpoint management software to securely configure systems?
  5. Does the department apply critical security patches as soon as practical or within 90 days of release?
- Notes - The IT Security Office provides departments with free access to the Center for Internet Security Configuration Assessment Tool (CIS-CAT) as well as BigFix endpoint management software. However, departments may elect to use other assessment and management tools such as Microsoft Baseline Security Analyzer and Ansible.

  Critical security patches should be applied within 90 days of release on all University systems. University Policy 7010, Policy for Securing Technology Resources and Services requires software updates for operating system and application software.

2.4 Continuous Vulnerability Assessment and Remediation

- Responsibility - University departments and the IT Security Office
- Methods
  1. Departments should provide the IT Security Office a list of critical systems and applications each year.
  2. The IT Security Office should conduct vulnerability assessments on critical systems and applications annually.
- Metrics
  1. Has the department provided the IT Security Office a list of critical systems and applications within the last year?
  2. Has the IT Security Office scanned critical systems and applications within the department during the last year?
- Notes - Unlike many organizations that have tightly controlled, centrally managed IT environments, Virginia Tech has many decentralized IT systems and networks managed by various departments, research groups and colleges. This dynamic, decentralized nature creates IT security monitoring challenges for the University.

  By providing a list of critical systems and applications to the IT Security Office, departments can help ensure that critical University IT assets are more closely monitored and scrutinized.

  The IT Security Office runs periodic port scans across the University's IP space and perform vulnerability scans upon request. In addition, IT Security monitors the Security Operations Center and conducts security reviews on critical VT systems and applications.

2.5 Malware Defenses

- Responsibility - University departments and the Division of Information Technology (DoIT)
- Methods
  1. Departments should scan and attempt to block email attachments and email links that appear malicious.
  2. Departments should configure host based firewalls to limit/restrict network connectivity.
  3. Departments should install and monitor antivirus software.
  4. Departments should send critical system logs to the DoIT's centralized log system.
  5. Departments should use the IT Security Office restricted DNS service.
- Metrics
  1. Does the department scan email for malicious attachments and links?
  2. Does the department properly configure host based firewalls?
  3. Does the department install and monitor antivirus software?
  4. Does the department send critical system logs to the DoIT's central log system?
  5. Does the department use the IT Security Office restricted DNS service?
- Notes - Departments that utilize the DoIT provided email services (Google Apps for Education and Microsoft Exchange) already receive email security mitigations.

  The DoIT provides Symantec Antivirus software for both Windows PCs and Macs at no cost to all faculty, students, and staff.

  In addition to the above listed methods, departments should consider further malware defenses such as Microsoft's Enhanced Mitigation Toolkit (EMET) for Windows operating systems and the Grsecurity kernel patches for Linux operating systems, etc.

2.6 Application Software Security

- Responsibility - University departments and the IT Security Office
- Methods
  1. Departments should ensure that applications are supported and maintained by the publisher.
  2. Departments should ensure that security patches are applied to applications in a timely manner.
  3. The IT Security Office should work with departments to conduct periodic vulnerability assessments, security reviews, and penetration tests of applications.
  4. Application developers and database administrators should receive annual role-based IT security training.
  5. Applications that accept user input should perform input validation and output sanitization.
  6. Departments should submit a list of important, business critical applications to the IT Security Office once a year.
- Metrics
  1. Does the department use only supported and maintained applications?
  2. Does the department ensure that security patches are applied to applications in a timely manner?
  3. Has the IT Security Office conducted a vulnerability scan, security review, or penetration test of critical departmental applications?
  4. Do application developers and database administrators within the department receive annual role-based IT security training?
  5. Do the applications perform input validation on all untrusted inputs and output sanitization?
  6. Last calendar year, did the department submit a list of business critical applications to the IT Security Office?
- Notes - For web application security, the IT Security Office urges all Departments to implement best practices discussed in the Open Web Application Security Project's (OWASP) Top 10 Project.

  The IT Security Office offers vulnerability assessments, security reviews, and penetration tests to University departments.

  Critical security patches should be applied as soon as practical, or within 90 days of release.

2.7 Wireless Access Control

- Responsibility - University departments and Network Infrastructure and Services
- Methods
  1. Departments must require unique user authentication before allowing devices to connect to wireless networks.
  2. Wireless networks must encrypt all traffic with at least WPA2 (AES).
- Metrics
  1. Does the department require unique user authentication before allowing a wireless connection?
  2. Does the wireless network encrypt all traffic with at least WPA2 (AES)?
- Notes - Currently, Virginia Tech allows faculty, staff and students to run wireless access points so long as those devices do not interfere with or interrupt the wireless service provided by Network Infrastructure and Services. However, all departments must be able to track and account for wireless network usage to address issues such as DMCA notices, IT security incidents, and misuse or abuse of the network.

  Departments that utilize the DoIT provided wireless network service (eduroam) already comply with the methods for this control.

2.8 Data Recovery Capability

- Responsibility - University departments and the Division of Information Technology
- Methods
  1. Departments should have periodic, automatic backups configured on all business critical systems.
  2. Departments should occasionally restore files from backup to ensure that the recovery procedure works and that the restored files contain the proper content.
  3. Departments should ensure that backups are encrypted at rest and in transit.
- Metrics
  1. Does the department automate backups on all business critical systems?
  2. Does the department periodically restore and test files from backup?
  3. Are the backups encrypted at rest and in transit?
- Notes - Network Infrastructure and Services provides a NAS that departments may use to backup important files. The NAS takes periodic, read-only snapshots that are resistant to ransomware attacks such as CryptoLocker. In addition to the NAS, departments may also leverage Tivoli Storage Manager as a backup solution. TSM can also be configured to encrypt backups.

2.9 Security Skills Assessment and Appropriate Training to Fill Gaps

- Responsibility - University departments and the IT Security Office
- Methods
  1. Departments should require all employees to complete security awareness training annually.
  2. Departments should require new employees to complete security awareness training within the first 30 days of employment.
  3. Departments should require all IT employees (technical and managerial) to attend annual role-based IT security training.
- Metrics
  1. Did the department's employees complete security awareness training during the last calendar year?
  2. Did new employees in the department complete security awareness training during the first 30 days of employment?
  3. Did the department's IT employees attend role-based IT security training during the last calendar year?
- Notes - The IT Security Office provides free online security awareness training to University departments. The IT Security Office also schedules and facilitates annual role-based technical security training through the SANS Institute. In addition to these training opportunities, University departments may request in-person training sessions through Service Now.

2.10 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

- Responsibility - University departments and Network Infrastructure and Services
- Methods
  1. Departments should use configuration management software to ensure security and consistency across devices as well as version control software to manage network device configurations.
  2. Departments should install the latest stable release of the network device firmware and/or operating system and also ensure that all critical security patches are applied in a timely manner.
  3. Departments should use encrypted sessions when connecting to and managing network devices.
  4. Departments should use dedicated management networks rather than the primary data networks when connecting to and managing network devices.
- Metrics
  1. Does the department use configuration management software and also store device configurations in a version control system?
  2. Does the department apply security patches to network devices in a timely manner and install the latest firmware?
  3. Does the department use encrypted sessions when connecting to and managing network devices?
  4. Does the department use separate, dedicated management networks to connect to and manage network devices?
- Notes - Configuration management software and version control software such as Mercurial or Git help ensure that devices are consistently configured and also allow for configuration backups and rollbacks when needed. Only encrypted protocols such as SSH should be used for network device management. Non-encrypted protocols such as Telnet and FTP should be disabled on all network devices. If there is no physically separate management network, departments may consider using dedicated management VLANs.

2.11 Limitation and Control of Network Ports, Protocols, and Services

- Responsibility - The IT Security Office and University departments
- Methods
  1. Departments should disable unneeded protocols and services that are not required for business purposes.
  2. Departments should enable and properly scope host-based firewalls on all systems.
  3. Departments should operate critical protocols and services (WWW, DNS, Mail, Database, etc.) on separate physical or separate logical hosts.
  4. The IT Security Office should conduct periodic port scans on critical University systems.
- Metrics
  1. Does the department disable unneeded protocols and services on all systems?
  2. Does the department enable and scope host-based firewalls on all systems?
  3. Does the department operate critical protocols and services on separate physical or separate logical hosts?
- Notes - Unneeded protocols and services such as FTP, Telnet, WWW, Mail, RDP, SSH, etc. may be enabled accidentally during software upgrades and installation.

  Properly scoped host firewalls allow only certain, authorized hosts to connect and disallow all other connections. Host firewalls may also prevent misconfigured or unneeded services from being exposed to network attacks.

  Running critical services on separate physical or separate logical machines enforces segmentation and isolates the services from one another.

  The IT Security Office conducts periodic port scans across the University's IP ranges.

2.12 Controlled Use of Administrative Privileges

- Responsibility - The Division of Information Technology and University departments
- Methods
  1. Departments should restrict access to administrative accounts and only use them when required to manage or configure systems.
  2. Departments should require administrative account passwords to be configured per the University's Password Rules.
  3. Departments should change all default administrative account passwords before deploying systems.
  4. Departments should ensure that all systems store administrative account passwords using the strongest hashing or encryption algorithm available to the system.
  5. Departments should require that each administrative account password is unique and not used on other account or systems.
  6. Departments should use multifactor authentication on all administrative accounts when possible.
- Metrics
  1. Does the department restrict access to administrative accounts and only use them when required?
  2. Does the department require administrative account passwords to abide by the University's Password Rules?
  3. Does the department change default administrative account passwords before deploying systems?
  4. Does the department store administrative account passwords using the strongest storage mechanism available?
  5. Does the department require separate, unique passwords on all administrative accounts?
  6. Does the department use multifactor authentication on all administrative accounts?
- Notes - A few examples of administrative accounts include, but are not limited to, root on Linux systems, Administrator on Windows systems and SYS on Oracle databases. The IT Security Office strongly encourage departments to use password managers to store administrative account passwords.

2.13 Boundary Defense

- Responsibility - The IT Security Office, Network Infrastructure and Services and University departments
- Methods
  1. Departments should require all remote logical access to use multifactor authentication.
  2. Department that process, store, or transmit Personally Identifiable Information (PII) should place hosts on the Restricted LAN (RLAN).
- Metrics
  1. Does the department require multifactor authentication for remote access?
  2. If the department handles PII data, does the department use the Restricted LAN for PII data processing?
- Notes - University departments may contact Secure Identity Services (SIS) about obtaining Duo integrations to provide multifactor authentication for remote access. Currently, the IT Security Office along with Network Infrastructure and Services employ a variety of Intrusion Detection and Prevention Systems as well as network flow monitoring systems.

  The IT Security Office and Network Infrastructure and Services actively monitor the University' network boundaries with Intrusion Detection and Prevention Systems (IDS and IPS) and record network flow data for forensic purposes.

2.14 Maintenance, Monitoring, and Analysis of Audit Logs

- Responsibility - The Division of Information Technology and University departments
- Methods
  1. Departments should configure all systems to use the University's NTP time servers.
  2. Departments should send logs to the DoIT's Log Archiving and Analysis (LAA) system.
  3. Departments should routinely monitor logs for anomalies.
- Metrics
  1. Does the department configure systems to use the University's NTP time servers?
  2. Does the department send logs to the DoIT's Log Archiving and Analysis system?
  3. Does the department routinely monitor logs for anomalies?
- Notes - Network Infrastructure and Services provide several high availability NTP time servers that departments may use. The University's NTP time servers are accessible from on or off campus. These servers are:
  - ntp-1.vt.edu
  - ntp-2.vt.edu
  - ntp-3.vt.edu
  - ntp-4.vt.edu

  When sending logs to the LAA system, departments should send all logs. Operating system logs, network device logs, application logs, database logs as well as other sources should be sent to the LAA system. Routine log monitoring may reveal system performance issues, misconfiguration, service failures, and security incidents.

2.15 Controlled Access Based on the Need to Know

- Responsibility - The Division of Information Technology and University departments
- Methods
  1. Departments that access Personally Identifiable Information (PII), should obtain and use Restricted LAN (RLAN) connections.
  2. Departments should encrypt PII data at rest and in transit.
  3. Departments that need additional Data Loss Prevention (DLP) solutions should use the IT Security Office's Active Directory Rights Management System (AD-RMS).
- Metrics
  1. If the department accesses PII, have RLAN connections been obtained and are they being used for PII data processing?
  2. Does the department encrypt PII data at rest (while stored) and in transit (during transmission)?
  3. If the department requires additional DLP, does the department use AD-RMS?
- Notes - Personally Identifiable Information includes U.S. social security numbers, passport numbers, drivers license numbers, credit card account information, debit card account information and bank account information. The University has established a Standard for Storing and Transmitting PII. The Restricted LAN (RLAN) was designed to segment PII data processing activities from non-PII data processing activities and has additional security layers in place. University departments that process, store, or transmit PII should contact the IT Security Office for information on joining the RLAN. AD-RMS allows departments to further restrict how documents may be used by providing the ability to limit or prevent operations such as copying, editing, printing, forwarding, and deleting documents.

2.16 Account Monitoring and Control

- Responsibility - The Division of Information Technology and University departments
- Methods
  1. Departments should periodically review and disable unused or dormant system accounts.
  2. Departments should establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.
  3. Departments should configure screen locks to protect unattended systems.
  4. Departments should configure systems to automatically log off users after a period of inactivity.
  5. Departments should require multi-factor authentication for accounts with access to sensitive data or elevated privileges.
- Metrics
  1. Does the department periodically review and disable unused or dormant system accounts?
  2. Does the department establish and follow a process for revoking system access by disabling accounts immediately upon termination?
  3. Does the department configure screen locks to protect unattended systems?
  4. Does the department configure systems to automatically log off users after a period of inactivity?
  5. Does the department require multi-factor authentication for accounts with access to sensitive data or elevated privileges?
- Notes - Departments may use BigFix, Active Directory Group Policy, Puppet, Ansible or some other centralized management system to automate many of these settings. Also, departments should note that some security standards require very specific settings. For example, the Payment Card Industry (PCI) requires automatic log off after 15 minutes of user inactivity. University departments may contact Secure Identity Services (SIS) about obtaining Duo integrations to provide multifactor authentication for accounts with access to sensitive data or elevated privileges.

2.17 Data Protection

- Responsibility - The Division of Information Technology and University departments
- Methods
  1. Departments should encrypt sensitive data at rest and in transit using NIST approved, publicly vetted encryption algorithms.
  2. Departments should perform annual assessments of business practices to identify practices that process, store and transmit sensitive information.
  3. Departments should perform periodic scans to locate and secure sensitive information.
- Metrics
  1. Does the department encrypt sensitive data at rest and in transit?
  2. Does the department perform annual assessments of business practices to identify sensitive information?
  3. Does the department perform periodic scans to locate and secure sensitive information?
- Notes - University Policy 7100 defines University employee roles and responsibilities with regard to data management and access. The University Standard for Storing and Transmitting PII defines and describes the requirements for dealing with sensitive data. For whole disk encryption, The IT Security Office recommends BitLocker for Windows Systems, FileVault for Macs and dm-crypt for Linux systems. The IT Security Office provides a site license for the Identity Finder client as well as the Identity Finder management console. Departments may download Identity Finder client from the Network Software website and the Identity Finder management console from Canvas.

2.18 Incident Response and Management

- Responsibility - The IT Security Office, University management and University departments
- Methods
  1. Departments should understand their role in the University incident response plan.
  2. Departments should have a written incident response plan to address department-specific, localized IT security incidents.
  3. Departments should conduct periodic IT security related incident response scenarios.
- Metrics
  1. Does the department understand their role in the University incident response plan?
  2. Does the department have a written incident response plan for localized IT security incidents?
  3. Does the department conduct periodic IT security incident response scenarios?
- Notes - Departmental incident response plans should have specific technical and management roles that are clearly defined. Knowing beforehand which individuals are responsible for communication, decision making, technical countermeasures, etc. will help ensure that University departments are prepared to handle actual IT security incidents. The University incident response plan is an overarching plan that is activated when an IT security incident has been identified as affecting University IT systems/services at an enterprise or multi-departmental level.

2.19 Secure Network Engineering

- Responsibility - Network Infrastructure and Services, the IT Security Office and University departments
- Methods
  1. Departments that process, store, or transmit Personally Identifiable Information (PII) should place hosts on the Restricted LAN (RLAN).
  2. Departments that manage network devices (routers, switches, firewalls, etc.) must be able to rapidly deploy access control lists and other defensive measures.
  3. Departments that manage network devices should use centralized configuration management software.
- Metrics
  1. If the department handles PII, have RLAN connections been obtained and are they being used for PII data processing?
  2. If the department manages network devices, does the department have the ability to rapidly deploy access control lists?
  3. If the department manages network devices, does the department use centralized configuration management software?
- Notes - In general, networks at Virginia Tech do not have network-based firewalls. However, the Restricted LAN (RLAN) was designed to segment PII data processing activities from non-PII data processing activities and has additional network security layers in place. University departments that process, store, or transmit PII should contact the IT Security Office for information on joining the RLAN.

2.20 Penetration Tests and Red Team Exercises

- Responsibility - The IT Security Office and University departments
- Methods
  1. Departments should provide the IT Security Office a list of critical systems and applications each year.
  2. The IT Security Office should conduct penetration tests against critical systems and applications annually.
- Metrics
  1. Has the department provided the IT Security Office a list of critical systems and applications within the last year?
  2. Has the IT Security Office conducted penetration tests against critical systems and applications within the department during the last year?
- Notes - Penetration tests should be carefully scoped and coordinated to ensure that they do not impact the department's business operations.

  In some cases, the IT Security Office may use vulnerability testing in conjunction with penetration testing to help guide penetration test efforts.

3 GLOSSARY

CIS-CAT:

Division of Information Technology (DoIT): Virginia Tech's central information technology organization www.it.vt.edu.

Fixed Assets: Virginia Tech's asset inventory department is part of the University Controller's office www.controller.vt.edu.

IT Security Office (ITSO): Virginia Tech's IT Security Office www.security.vt.edu.

Penetration Test:

Restricted LAN (RLAN):

University department: A catch-all term that refers to various divisions, departments and areas at Virginia Tech. Sometimes shortened to the word 'department'.