Top 10 Minimum Security Controls

Introduction
Altius IT's list of minimum security controls is based upon security best practices. This list may not be complete and Altius IT recommends this list be augmented with additional controls. While not all risk can be eliminated, security controls include preventive, detective, and corrective safeguards that help reduce risks to acceptable levels.

1. Patches and Updates
Vendor-issued critical security updates and patches are applied in a timely manner to protect data and systems. These include servers, workstations, firewalls, network switches and routers, mobile devices, software applications and related technologies.

2. Anti-malware Protection
Anti-malware software protects systems and applications. Procedures and tools guard against, detect, and report malicious software. Centrally managed anti-malware software continuously monitors and protects information systems. Ensure anti-malware protection mechanisms are updated in a timely manner.

3. System and Data Backups
Robust backup solutions enable the recovery of data and applications in the event of natural disasters, system disk drive failures, espionage, data entry errors, viruses, or system operations errors.

4. Strong Authentication
Strong authentication mechanisms are implemented and maintained. User roles should be defined based on the principle of "least privilege". If a user role will not be modifying data, then the role should not be given the opportunity to edit, delete, or add data. Multi-factor authentication is required for remote access to the network and privileged or administrative access.

5. Encryption
Determine data that is critical or vulnerable and develop encryption schemes to protect the data from unauthorized users and use. Sensitive data should also be encrypted while in transit and when stored.

6. Security Training and Awareness
Security-related training is provided to all staff and customized to their specific roles and job duties. Security training is performed at time of hire, after a leave of absence, and on an annual basis. Security awareness is performed several times a month and may include e-mail reminders, posters in break rooms, discussions during staff meetings, etc.

Top 10 Minimum Security Controls

7. Logging and Monitoring
System events and activities should be monitored and logged. Actions should be auditable where all activities that affect user state are formally tracked. Activity should be traceable to determine where and when an activity occurred and with high integrity where the logs cannot be overwritten or altered. Copies of log files should be made at regular intervals and log files should be copied to a protected area and retained to assist in future investigations and monitoring.

8. Third-party service providers and supply chain
Identify risks related to third parties and supply chains. Establish third-party and supply chain responsibilities and implement controls to protect systems and data.

9. Incident Response Plan and Business Continuity Plan
Incident Response Plans protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. Incident Response Teams are trained to identify and report incidents, perform initial investigations, determine risk classification, document and communicate incidents, perform appropriate response procedures, and provide incident reporting.

Business Continuity Plans provide mechanisms that allow an organization to continue business operations in the event of a disaster or component failure. Business continuity identifies risks and implements the appropriate mitigating technologies and processes..

10. Security audits
Independent security audits verify security controls are sufficient and efficient. Security audits are performed on an annual basis and when there is a major change in the environment.

Publication Information
Altius IT is a security audit, security consulting, and risk management firm. We are certified by the Information Systems Audit and Control Association (ISACA) as a Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), and Certified in the Governance of Enterprise Wide IT (CGEIT). For more information, please visit www.AltiusIT.com.