# IT Infrastructure Information Security Best Practices

PONDURANCE

***The information contained herein is intended to provide common recommendations and is developed for informational purposes only. This guide is not designed to be comprehensive, and some recommendations may not be suitable to an organization based on its requirements and integration with additional business applications.***

## NETWORK PERIMETER HARDENING

**Attack surface -** Regularly run external vulnerability scans against your external facing IP address(es). This will assist with limiting your network's exposure to the internet and inform you of vulnerabilities or insecure configurations that may put your network at risk. External scans should be run on a quarterly basis and/or whenever a configuration change occurs on the network.

**Remote access channels -** Any methods of remote access to your network infrastructure (virtual private network (VPN), virtual desktop infrastructure, FTP/SFTP, etc.) should be restricted by establishing role-based permissions and protected with additional secure authentication methods (multifactor authentication (MFA), trusted devices, geolocation, etc.).

**Network segmentation -** Servers hosting externally available services should be logically segmented from the rest of the network by placing them in a demilitarized zone, with restricted firewall rules only allowing protocols that are necessary for business operations. This will reduce the potential impact of a server compromise due to service vulnerability or misconfiguration.

**NAT and proxy servers with firewalls -** Configure a proxy server on your gateway with network address translation (NAT) and firewalls to share the internet connection securely for your local area network (LAN). Block IP addresses and networks known to be malicious. Prevent users from connecting personal devices, such as phones, for internet access on your main network.

## INTERNAL NETWORK HARDENING

**Asset inventory -** Maintain a current inventory of every asset that is connected to the network. A good security posture starts with an accurate inventory of all assets on the network. You cannot protect what you don't know exists.

**Network isolation -** As much as possible, segment networks according to roles, criticality, and risk. Restrict network traffic between virtual LANs to only what is necessary.

**SMB hardening -** Disable Server Message Block (SMB) version 1 and block all versions of SMB at the network perimeter. Enable SMB signing and extended protection for authentication, if the infrastructure allows.

**Authentication protocols -** Disable New Technology LAN Manager (NTLM) version 1 and LM protocols. If required, enable NTLM authentication auditing and set exclusions for business-critical systems prior to blocking NTLMv1 for the rest of the network. Ensure that only authorized and authenticated users can access SMB/Common Internet File System shares on the network (e.g., deny access to "everyone" and "anonymous logon" groups). Require network level authentication for remote desktop connections and disallow remote desktop protocol (RDP) traffic unless necessary.

**Control open RDP -** RDP should only be open to internal IP addresses and not accessible over the internet. If external RDP access is required, it should be routed through a VPN that is configured to acceptable standards. Older VPN protocols, such as point-to-point tunneling protocol, should be avoided.

**Network access control -** Implement physical access controls to prevent unauthorized devices from accessing enterprise networks, such as 802.1x.

**AppData/Temp folders -** Restrict file types that can run from the AppData and Temp folders. Configure a group policy to restrict file types that are allowed to run from these folders.

## SYSTEM HARDENING AND MANAGEMENT

**Network footprint reduction -** Ensure the firewalls are enabled and configured to only allow access to necessary ports.

**Centralized remote monitoring and management (RMM) -** Implement a centralized monitoring and management solution to allow for effective inventory administration and scalable deployment. Monitor network assets to ensure RMM coverage for all assets on the network and review software inventory to identify unauthorized applications. Develop and implement a detection strategy for unauthorized devices on the network.

**IT life cycle management -** Create a standardized process of IT asset acquisition to include provisioning devices with a standard software baseline. Monitor the software and health of IT assets throughout the device's life cycle. Identify the software, operating system, and hardware end-of-life support dates and plan for the disposal or isolation of systems as they transition to legacy status.

**Local admin account controls -** Implement a local administrator account and password management solution to mitigate the potential impact of the compromise of a system.

**Data protection -** Encrypt computer systems to mitigate the potential impact of workstation loss or theft. Ensure that encryption recovery keys are appropriately escrowed to allow for system access and data recovery in the event of an employee's departure or a forgotten password.

**Legacy data -** Data should be audited regularly for relevancy. When data is no longer needed, it should either be archived offline or deleted, based on your data retention requirements.

**Backups -** Ensure that backups are being tested and restored on a regular basis to ensure proper backup and recovery processes are being followed. Data backups should be stored offline and not be accessible through credentials stored within the active directory (AD).

**Application whitelisting -** Whitelisting websites and applications can prevent unauthorized downloading and execution on a network.

## IDENTITY AND ACCESS MANAGEMENT

**Password complexity -** Enforce password complexity requirements for all network accounts.

**Account life cycle management -** Ensure that proper onboarding and offboarding policies and procedures are documented and regularly audited. Monitor active accounts for any unauthorized account creations or modifications.

**Administrative access controls -** Implement MFA for any privileged accounts (administrative accounts, etc.). Regularly audit logons and access using privileged accounts to identify potential misuse. Systems administrators should use a separate unprivileged account for regular activity (e.g., email, individual workstation access).

**Least privilege policy -** Deny administrative privileges to users unless required. Only allow users access to file shares, servers, etc. that are necessary for their specific roles.

**Break glass account -** Create a privileged account with elevated permissions to be used only in the event of an emergency that can circumvent regular controls. Set a strong password and retain the password in an out-of-band location (i.e., locked safe). Additionally, implement a protocol for break glass account use and detection rules to alert all stakeholders in the event of account use.

**Minimum security policy -** Enforce a minimum-security standard and requirement to connect to networks and resources across the organization. Implement a solution to audit a device's security prior to connecting.

**MFA device auditing -** Audit devices/applications in use by each user for MFA implementation and proper configuration.

**Single sign-on (SSO) -** Microsoft includes a number of security features within the Azure AD environment that facilitate integration across platforms. Consider the vast number of business email compromises that occur and how compromised credentials for email accounts have the potential to be leveraged for unauthorized access to other applications that use AzureAD SSO.

**User account control (UAC) -** Configure UAC to the most restrictive settings possible to continue normal business practices. When specific trusted programs require administrative privileges, a scheduled task can be created to run as the administrator without the need for the user to have local administrative rights.

## MONITORING AND RESPONSE

**Log aggregation -** Implement a log aggregation and retention solution to allow for centralized access to existing application and operating system logging. Ensure that the retention period is sufficient to cover any potential regulatory requirements. Monitor logs for anomalous or malicious activity.

**Host and network monitoring -** Implement an endpoint detection and response (EDR) solution to monitor system activity that will provide proactive system protection and quickly identify potential incidents. Implement a network monitoring solution to monitor network traffic and identify anomalous traffic. Regularly review EDR and network monitoring logs for alerts and indicators of compromise. Ensure that EDR is installed on all systems in your environment and is monitored and configured to avoid alert fatigue.

**24/7 security operation center (SOC) monitoring -** A 24/7 SOC-monitored network will provide the quickest response to any incident. Trained analysis can proactively seek out threats and quickly respond to identified threats within the environment.

**Incident response plan -** Create and implement a formal incident response plan to include actions taken after detection of a potential incident. The incident response plan should include notification guidelines and steps for recovery actions and allow for a post-incident review for various categories of incidents.

**Tabletop exercises -** Conduct tabletop exercises on a regular basis. Testing the incident response plan with tabletop exercises is the best way to ensure the organization is prepared when an incident occurs. Testing will also identify potential blind spots within the plan that can be addressed to ensure an effective response.

## VULNERABILITY MANAGEMENT

**Scanning and patching -** Implement a vulnerability scanning solution to identify vulnerable systems and unauthorized devices on the network. Implement a patch schedule with approved downtime periods. Monitor software vendor news feeds for notification of significant vulnerabilities and implement an emergency patch policy for high-risk vulnerabilities.

**Legacy system management -** Implement a mitigation strategy for business-critical systems that are out of support and pose a risk to the network. Track support periods for operating systems, software, and hardware and proactively implement mitigation strategies (e.g., network isolation).

## HOW PONDURANCE CAN HELP

***Our mission is to ensure that every organization is able to detect and respond to cyber threats — regardless of size, industry, or current in-house capabilities. We combine our advanced platform with decades of human intelligence to decrease risk to your mission.***

### CLOSED-LOOP MANAGED DETECTION AND RESPONSE

Recognized by Gartner, Pondurance provides 24/7 U.S.-based SOC services powered by analysts, threat hunters, and incident responders who utilize our advanced cloud-native platform to provide you with continuous cyber risk reduction. By integrating 360-degree visibility across log, endpoint, and network data and with proactive threat hunting, we reduce the time it takes to respond to emerging cyber threats.

Pondurance Managed Detection and Response is the proactive security service backed by authentic human intelligence. Technology is not enough to stop cyber threats. Human attackers must be confronted by human defenders.

### INCIDENT RESPONSE

When every minute counts, organizations need specialized cybersecurity experts to help them respond to a compromise, minimize losses, and prevent future incidents.

Pondurance delivers digital forensics and incident response services with an experienced team capable of assisting your organization and legal team every step of the way. This includes scoping and containing the incident, determining exposure through forensic analysis, and providing confidence to continue normal business operations.

### SECURITY CONSULTANCY SERVICES

Our specialized consultancy services will help you assess systems, controls, programs, and teams to uncover and manage vulnerabilities. Our suite of services ranges from Penetration Testing to red team exercises, along with Compliance program assessments for highly regulated industries. We provide security incident response and business continuity planning to put you in the best position to defend against and respond to cyberattacks.

## CONTACT US

**Emergency Incident Response Hotline: 888.385.1720**
**Email: dfir@pondurance.com**

**pondurance.com**