**Secure System Baseline Guide**

**1. What Is a Secure System Baseline and Why Is It Critical?**

A **secure system baseline** is a documented set of minimum-security configurations and practices that every system in an organization must adhere to. It defines a “known good state” for devices and platforms, ensuring that security settings are uniformly applied and maintained. For small businesses—often constrained by limited budgets and IT resources this baseline is critical because it:

* **Ensures Consistency:** Establishes uniform security measures across all systems, reducing vulnerabilities from misconfigurations.
* **Simplifies Compliance:** Provides a clear reference for meeting regulatory and industry standards (e.g., NIST SP 800-53, CIS Benchmarks).
* **Reduces Risk:** Minimizes exposure to cyber threats by enforcing essential security controls from the start.
* **Enhances Efficiency:** Enables quick deployment, easier maintenance, and rapid response to emerging threats.

*Simple Explanation:* Think of it as a safety checklist for all your devices that makes sure every computer or network device is set up securely from the start.

**2. Baseline Security Configuration Document**

This section outlines the key security settings for different types of systems. Two versions are provided: a **detailed version** for technical teams and a **simplified version** for non-technical users.

**A. Windows Systems**

**Detailed Version:**

* **Firewall:**  
  • Enable Windows Firewall with predefined rules for inbound and outbound traffic.
* **Automatic Updates:**  
  • Configure Windows Update to install critical patches automatically.
* **Antivirus:**  
  • Install and maintain up-to-date antivirus software with real-time scanning enabled.

**Simplified Version:**

* **Firewall On:**  
  Think of it as a security guard watching your computer traffic.
* **Automatic Updates:**  
  Let your computer install updates automatically like regular check-ups.
* **Antivirus Software:**  
  Use trusted antivirus software to catch and remove viruses.

**B. Linux Systems**

**Detailed Version:**

* **User Access:**  
  • Disable direct root logins and require the use of sudo for administrative tasks.
* **SELinux:**  
  • Enable SELinux in enforcing mode for an extra layer of access control.
* **SSH Restrictions:**  
  • Configure SSH to disable password-based authentication in favor of key-based authentication.  
  • Limit SSH access to specific IP addresses and change the default SSH port if possible.

**Simplified Version:**

* **No Direct Admin Logins:**  
  Instead of logging in as the “boss” (root), use a regular account and ask for permission when needed.
* **Enable SELinux:**  
  This adds an extra shield that controls what programs can do.
* **Secure Remote Access:**  
  Use a secret key instead of a password for remote access and only allow trusted users.

**C. Cloud Platforms**

**Detailed Version:**

* **Access Controls:**  
  • Implement robust Identity and Access Management (IAM) policies with role-based access and multi-factor authentication.
* **Logging:**  
  • Enable comprehensive logging (e.g., CloudTrail for AWS) to monitor user activities and system changes.
* **Encryption:**  
  • Ensure that all data stored in the cloud is encrypted at rest and data in transit is secured using TLS 1.2 or higher.

**Simplified Version:**

* **Access Controls:**  
  Only allow the right people to access your data, like a locked door that only opens for authorized personnel.
* **Logging:**  
  Keep a record of who accessed or changed your data.
* **Encryption:**  
  Encrypt your data so that even if someone gets hold of it, it remains unreadable.

**D. Network Devices (Routers, Switches, Firewalls)**

**Detailed Version:**

* **Service Management:**  
  • Disable all unnecessary services and protocols (e.g., Telnet, FTP) that are not needed.
* **Authentication:**  
  • Enforce strong, unique passwords and use secure management protocols (e.g., SSH instead of Telnet).
* **Firmware Updates:**  
  • Regularly update firmware to protect against known vulnerabilities and ensure vendor patches are applied promptly.

**Simplified Version:**

* **Disable Unnecessary Services:**  
  Turn off features you don’t need—like closing unused doors.
* **Strong Authentication:**  
  Use strong, unique passwords and, if possible, add a second layer of security (two-factor authentication).
* **Regular Firmware Updates:**  
  Keep your device software updated to fix security holes.

**3. Patch Management Policy**

**Detailed Version:**

**Objective:**  
Maintain the security and functionality of all systems by applying regular updates and patches and tracking these changes in an asset management log.

**Policy Guidelines:**

* **Regular Updates:**  
  – Schedule automatic or manual updates for all systems (Windows, Linux, cloud environments, and network devices) on a predefined cycle (e.g., weekly or monthly).
* **Patch Verification:**  
  – Test patches in a controlled environment before full deployment to minimize operational disruptions.
* **Asset Management Log:**  
  – Record each patch installation with details such as asset ID, patch details, date applied, and responsible technician.  
  – Reference NIST SP 800-53 controls (e.g., CM-8, CM-8(1)) to ensure compliance.
* **Monitoring and Reporting:**  
  – Continuously monitor patch levels and generate periodic compliance reports to ensure all systems remain within the secure baseline.

**Simplified Version:**

* **Regular Updates:**  
  Make sure all your devices are updated regularly (set a weekly or monthly schedule).
* **Test Updates First:**  
  If possible, try out updates on a small group of devices to avoid problems.
* **Keep a Simple Record:**  
  Use a spreadsheet or checklist to note:
  + What was updated
  + When it was updated
  + Who did the update

**4. Asset Maintenance Policy**

**Detailed Version:**

**Objective:**  
Establish a clear process for managing the lifecycle of IT assets—from acquisition and regular maintenance to repair and decommissioning.

**Policy Guidelines:**

* **Asset Documentation:**  
  – Maintain a detailed inventory of all IT assets (hardware, software, and cloud resources) with unique identifiers, acquisition dates, and assigned responsibilities.
* **Maintenance Logging:**  
  – Log all repair activities, configuration changes, and updates to each asset. Include details such as date, description of work, and technician name.
* **Update and Repair Tracking:**  
  – Ensure that any updates or patches are cross-referenced with the patch management log. Schedule periodic reviews to determine if repairs or upgrades are needed.
* **Decommissioning Procedures:**  
  – Document the process for retiring assets, ensuring sensitive data is securely wiped or migrated. Update the asset log to reflect decommissioned items.
* **Compliance and Audits:**  
  – Regularly audit asset logs to ensure maintenance and decommissioning procedures meet compliance requirements.

**Simplified Version:**

* **Inventory List:**  
  Keep a simple list of all your devices (computers, routers, etc.).
* **Log Repairs and Updates:**  
  Record every repair, update, or change made to each device.
* **End-of-Life Procedure:**  
  When a device is retired, remove any sensitive data and update your list to show it’s no longer in use.