CONNECTWISE
Access-Management

Privileged Access Policy Checklist

10 Steps to Building More Secure Access Management

Ever wonder who's really knocking on your digital doors? To ensure the utmost security, take control and fortify defenses with a privileged access policy that improves access management and keeps unwanted intruders at bay.

Follow these 10 steps to build your own policy:

1. **Understand Business Requirements and Regulatory Compliance**
   Determine relevant industry regulations and compliance standards for your business or customers.

2. **Define Privilege Levels for Accounts and Users**
   Find all privileged accounts and users within your managed systems and define levels with the principle of least privilege (POLP) so users can only access systems required for their responsibilities.

3. **Inventory Systems and Assets**
   To help map privileges to specific resources, create an inventory of all systems, assets, applications, and data your team is responsible for managing.

4. **Implement RBAC and Access Approval Processes**
   Implement a role-based access control system (RBAC) to assign privileges based on job roles and responsibilities. Then, establish an access approval process that requires proper authorization and documentation before granting privileged access.

5. **Set Password Management Standards**
   Set standards in password complexity to ensure passwords are strong and unique. Implementing a password management system or more modern tools that allow for "passwordless" access will help you better manage privileged account and device access.

6. **Regularly Review Your Policy and Incident Response Plan**
   Regularly review and update your privileged access policy to ensure it remains aligned with the evolving cybersecurity landscape. Additionally, develop an incident response plan specifically tailored for handling breaches or unauthorized access to privileged accounts.

7. **Create Standards for Vendors**
   Ensure that the third-party vendors or subcontractors you engage with also adhere to your privileged access policy and security standards.

8. **Build Testing and Validation Processes**
   Conduct periodic penetration testing and cybersecurity assessments to identify vulnerabilities and weaknesses in your IT environment.

9. **Include Auditing and Monitoring Processes**
   Set up robust logging and monitoring mechanisms to track privileged access activities. Implement intrusion detection systems (IDS) and security information and event management (SIEM) tools to detect and respond to suspicious activities.

10. **Document, Communicate, and Train**
    Document your privileged access policy (including procedures, guidelines, and responsibilities), clearly communicate policy to all relevant stakeholders, and provide comprehensive training to employees.

Additional Access Management Resources

Privileged Access Management Best Practices >>

Principle of least privilege: definition, benefits, and more >>

CISA's Cyber Essentials Toolkit (US) >>

Cyber Essentials: Requirements for IT infrastructure (UK) >>

ACSC Essential 8 (AU) >>

CONNECTWISE

ConnectWise Access Management Free Trial >>