

Access Management & Procedures

Access Management Procedures

- A procedure detailing how access rights are assigned, reviewed, changed, and revoked. This should cover who is authorized to grant access, how access requests are validated, and how often access rights should be reviewed.

Software and Systems Update Standards

- Regular updates to systems and software applications are crucial in maintaining security. A standard can be set for timely updates and patches to mitigate vulnerabilities.

By Lucas Higgs

Access Management Procedures: (*Access management policy 2022*)

Background

Access to the Enterprise's electronic information resources must be managed in a manner that maintains the confidentiality, integrity, and availability of Enterprise resources, and in a manner that complies with any applicable legal and regulatory requirements.

Definitions

- Authentication: The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
- Authorization: Access privileges granted to a user, program, or process or the act of granting those privileges
- Multi-Factor Authentication (MFA): Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., token generation device); or (iii) something you are (e.g., biometric).
- Least Privilege: The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
- Privileged Access Management (PAM): The process of managing and protecting credentials to accounts that have some level of administrative access to devices or systems, including local administrator accounts and superusers.
- User: Individual or (system) process, acting on behalf of an individual, authorized to access a system
 - Organization User: An organizational employee or an individual whom the organization deems to have equivalent status of an employee, including a contractor, guest researcher, or individual detailed from another organization.

- Non-Organization User: A user who is not an organizational user
- Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Policy Statement

Access Management is the process of identifying, tracking, controlling, and managing user access rights to information systems. Any user who requests access to systems, applications, or data, must have their identity authenticated. Additionally, user access should be further restricted following the principle of Least Privilege, and in alignment with any Enterprise defined segregation of duties guidelines.

User account provisioning must include creation of unique credentials for new users and disablement and revocation of a terminated user's access privileges upon termination.

Privileged access must only be provided to users as needed. Users with privileged user accounts must also have an organizational user account, which follows the principle of least privilege, and must use this organizational user account for their day-to-day job functions. Privileged user accounts must only be used when elevated privileges are required by the system or application.

Where there is any requirement for shared usage of an account this must be signed off by the IT Security division and all usage must be audited and traceable to an individual authorized user account.

All remote access to the Enterprise's network must utilize a secure solution, which employs multi-factor authentication, and a secure network encryption protocol.

Multi-Factor Authentication

The Office of Information Technology has taken several steps to protect and monitor our Information Systems. As part of its efforts, the OIT has enabled Multi-Factor Authentication which provides a common method of protection for companies like ours, that utilize and store sensitive, personal, and financial information.

Access Management Procedures ChatGPT:

Access management procedures for a nonprofit organization are designed to ensure the security and integrity of the organization's systems, data, and resources while enabling authorized individuals to fulfill their roles effectively. Here are some key considerations for access management procedures in a nonprofit organization:

1. User Roles and Permissions: Clearly define user roles within the organization based on job responsibilities and functions. Assign appropriate access permissions to each role to ensure the principle of least privilege. Limit access to sensitive data or critical systems only to individuals who require it for their work.

2. **User Authentication:** Implement strong authentication mechanisms to verify the identity of users accessing the organization's systems. This can include the use of secure passwords, two-factor authentication, or biometric authentication methods, depending on the organization's resources and requirements.

3. **User Account Management:** Establish procedures for creating, modifying, and terminating user accounts. Ensure that new accounts are created for authorized individuals only, and promptly remove access for employees or volunteers who leave the organization. Regularly review and update access privileges to reflect any changes in roles or responsibilities.

4. **Data Access Controls:** Apply access controls to protect sensitive data. Utilize encryption techniques to secure data at rest and in transit. Implement data classification to identify and categorize data based on its sensitivity, allowing for more granular access controls.

5. **Regular Access Reviews:** Conduct periodic access reviews to ensure that access privileges align with current job roles and responsibilities. Remove unnecessary or outdated access permissions promptly to minimize the risk of unauthorized access.

6. **Training and Awareness:** Educate employees, volunteers, and stakeholders about the importance of access management and cybersecurity best practices. Provide training on password security, recognizing phishing attempts, and handling sensitive information appropriately.

7. **Monitoring and Logging:** Implement monitoring and logging mechanisms to track user activities, detect unauthorized access attempts, and identify potential security incidents. Regularly review logs for anomalies or suspicious behavior.

8. **Incident Response:** Establish an incident response plan to address security incidents promptly. Define procedures for reporting and handling security breaches, including unauthorized access attempts, data breaches, or compromised user accounts.

9. **Third-Party Access:** If the nonprofit organization works with external partners or vendors, establish guidelines for granting and managing their access. Implement contracts or agreements that outline access requirements, data protection measures, and accountability.

10. **Compliance with Regulations:** Ensure that access management procedures align with applicable data protection and privacy regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), depending on the organization's jurisdiction and activities.

Remember, access management procedures should be regularly reviewed, updated, and communicated to all relevant stakeholders to maintain their effectiveness and address any emerging security risks or changes in organizational structure.

Software and Systems Update Standards: (Bingham, 2022)

- Knowing your network, systems, devices, software, and users is first on this list because you can't adequately plan out software update deployments without this information.
 - Here's some of the essential information you should know about your IT environment:
 - The makes and models of the hardware devices on your network
 - Utilized operating systems
 - Utilized applications
 - Network structure and resources
 - Hours of operation
 - Critical systems
 - Users
 - VIP users
 - Security concerns
- While this may seem like a lot of information to gather, many available systems can manage the task for you.
 - For example, PDQ Inventory is a device management platform that automatically scans your network for Windows devices, gathering, organizing, and centrally storing detailed system configuration information for you. It can take care of getting to know your devices and systems while you get to know your users and their needs.
- Stay informed
 - While some systems release updates on a pretty regular basis, for example, Microsoft and Adobe release updates on Patch Tuesday (the second Tuesday of every month), other systems don't have a steady release schedule. Even Microsoft and Adobe frequently release out-of-band security patches to address vulnerabilities.
 - To help stay informed about the latest software updates, consider subscribing to RSS feeds, following developer social media accounts, and signing up for mailing lists for systems you utilize.
- Compliance standard requirements
 - Many organizations must adhere to specific standards to meet regulatory requirements, such as PCI DSS and SOC 2. Some regulatory standards require

deploying software updates within a particular time frame of release. Identifying which compliance standards your organization is required to meet will help you plan your patch deployment schedule.

- Develop a schedule that works for your organization
- Once you've gotten to know your IT environment and your regulatory requirements, it's time to develop a software patch deployment strategy that works for your organization. This step is often the most difficult because of the substantial number of factors to consider.
- Since each organization is unique, there is no one-size-fits-all approach to developing a deployment schedule, but here are a few tips to help out:
 - Don't deploy updates that require restarts during the middle of the day. This practice is considered *full contact IT*, and it is generally frowned upon — by users at least.
 - Establish a maintenance window that doesn't conflict with peak operation hours and heavy network traffic periods.
 - Some updates, like Microsoft Windows feature updates, can lock down a system for a considerable amount of time. Consider deploying these types of updates after regular business hours.
 - Divide your systems into preview, broad, and critical software update groups. The preview software update group is your tester group, which should receive updates shortly after release. The broad group should consist of the majority of your systems. These systems should receive patches after testing is complete. Essential systems belong in the critical software update group and should receive patches once they've been thoroughly tested and potentially delayed indefinitely if there are compatibility issues.
- Be Transparent
 - Once you've nailed down the perfect patch deployment schedule, inform your users of when to expect updates and their potential impact on their system. The workforce is a pretty tech-savvy bunch these days. Most users have a basic understanding of software updates and what it means for their systems. Keeping them informed builds trust.
 - If you ever get users complaining about updates, remind them of the risks associated with vulnerabilities and the consequences of a security breach. This info usually helps them understand why we do what we do.
- Be Ready to Adapt

- Certain patches, such as Microsoft's updates, you can count on. Every Patch Tuesday, they'll become available to the masses. Other updates, however, aren't as routine.
- IT teams need to be able to adapt and respond to patching needs, especially when a zero-day vulnerability is disclosed. Vendors take critical vulnerabilities very seriously and release patches ASAP. Ensuring your IT team can properly respond to out-of-band and last-minute critical software updates is an essential part of securing your organization's digital assets.
- Servers require special care
 - Servers are often a crucial part of an organization's IT infrastructure. As such, always take extra caution when updating servers. Windows Server receives cumulative updates every Patch Tuesday, just like its desktop OS counterpart. Consider delaying server patches for several days. This gives the tech community time to report any unintended behaviors or compatibility issues introduced by the updates. However, if a server is exposed because of a critical vulnerability, immediate patching is always recommended, though I'd still suggest doing it after hours — just in case.
- Proper testing saves you time and energy
- One of the most important aspects of deploying software updates is properly testing them before distributing them to the masses. Properly testing patches will save you a ton of time and aggravation if a problematic update needs to be uninstalled. Here are a few things to consider when establishing your testing process:
 - Send out patch deployments to your test machines and users as quickly as possible. This gives your testers adequate time to thoroughly test updates before they need to be deployed to your broad group.
 - Your test group should include a subset of machines that reflects the diversity of your organization's assets as a whole.
 - Enlist test users that are more likely to provide relevant and informational feedback.
 - Keep your test group small enough that if a problem patch is distributed, it's easy to remove.
- Automate to stay up to date
 - Sysadmins have a lot of responsibilities on their plates. Often, the only way for them to reliably distribute patches across thousands of devices and systems is to

use patch management software to automate the process. A patch manager solution can utilize automatic deployment rules to distribute updates across an organization. While various solutions provide this functionality, few products make it as easy as PDQ Deploy. Sysadmins struggling to keep up with their patch management needs can download a free 14-day trial to see for themselves how easy deploying patches can be.

- Audit your deployments
 - Auditing ensures updates are being deployed successfully and you don't have systems on your network that are missing patches. One system left with an unpatched vulnerability is all it takes for a bad actor to access your organization's network and assets.
 - To help your audits run smoothly, look for tools that provide intelligent reporting features, such as PDQ Deploy and Inventory. PDQ allows you to configure auto reports, ensuring you have all the information you need whenever you need it.

ChatGPT Software and systems update standards:

Nonprofit organizations, like any other entities, can benefit from following software and systems update standards to ensure the security, stability, and efficiency of their operations. Here are some common standards and best practices for software and systems updates in nonprofit organizations:

1. Regular Patch Management: Implement a patch management process to keep software and systems up to date with the latest security patches, bug fixes, and updates. This includes operating systems, applications, and firmware.
2. Software Version Control: Maintain a centralized repository or version control system to manage software versions and track changes. This helps ensure that the organization is using the latest stable versions of software and enables easy rollback if necessary.
3. Change Management Process: Establish a formal change management process to evaluate, approve, and implement updates. This process should include testing updates in a controlled environment before deploying them to production systems.
4. Scheduled Maintenance Windows: Define regular maintenance windows or downtime periods during which system updates and maintenance activities are performed. Communicate these windows to staff and stakeholders to minimize disruption.
5. Vendor Notifications: Stay informed about software and system updates by subscribing to vendor notifications and security mailing lists. This helps to receive timely information about vulnerabilities, patches, and updates relevant to the organization's technology stack.
6. Security Updates and Vulnerability Management: Stay proactive in addressing security

vulnerabilities by regularly scanning systems for vulnerabilities, using tools like vulnerability scanners. Promptly apply security updates and patches to mitigate potential risks.

7. Backup and Disaster Recovery: Implement a robust backup strategy to protect data and ensure business continuity. Regularly test backups and ensure the ability to restore systems in case of failures or security incidents.

8. Documentation and Knowledge Sharing: Maintain up-to-date documentation of software and systems configurations, update processes, and related procedures. This documentation aids in knowledge sharing, troubleshooting, and facilitating smooth transitions during staff turnover.

9. User Awareness and Training: Educate staff and users about the importance of software and systems updates, including the potential risks of neglecting updates and how to report issues. Promote a culture of security and compliance within the organization.

10. Monitoring and Performance Optimization: Implement monitoring tools and practices to track system performance, identify bottlenecks, and proactively address issues. Regularly review system logs and performance metrics to detect anomalies or indicators of potential problems.

It's important to note that the specific standards and practices may vary depending on the size, complexity, and budget of the nonprofit organization. It's recommended to consult with IT professionals or consider industry-specific frameworks, such as the NIST Cybersecurity Framework, for additional guidance.

Resources:

- *Access management policy*. St. George's University. (2022, April 12). <https://www.sgu.edu/office-of-information-technology/computing-policies/access-management/#:~:text=Policy%20Statement,must%20have%20their%20identity%20authenticated>.
- Bingham, B. (2022, March 22). *10 best practices for deploying software updates*. PDQ. <https://www.pdq.com/blog/deploying-software-best-practices/>