NC Department of Health and Human Services

Information Technology Division
Privacy and Security Section

May 16, 2025

The DHHS Privacy and Security Office

- The Privacy and Security Office (PSO) provides privacy and security information for the Department of Health and Human Services (DHHS). The PSS safeguards information from unauthorized use, disclosure, modification, damage or loss.
- The PSO provides consulting services around Privacy and Security, Business Continuity Planning (BCP), Continuity of Operations (COO), Disaster Recovery (DR), Forensic Investigations, Privacy and Security Policies, Incident Management, Risk and Threat Management.
- The PSO serves as the liaison between various Federal and State Agencies.
- The PSO is responsible for conducting annual reviews based on Federal and State requirements.

The DSS Quarterly Access Control Reposting

Organizations need to know who the admin users are for desktop, servers, mainframe applications, distributed applications, databases are and verify the access rights for regular users for all systems and applications.

Understanding Security Controls

Security controls are measures and mechanisms put in place to protect information systems from security threats, vulnerabilities, and risks

Management Based Controls

- Focus on policies, procedures, and organizational structures to manage risk and ensure information security
- Includes incident response, access control, and service provider management, program management

Operational Based Controls

- Focus on the actions and procedures used to protect systems and data during day-to-day operations
- Includes access control, change management, and monitoring, ensuring a secure environment.

Technical Based Controls

- Focus on measures implemented through hardware and software to protect systems, networks, and data from cyber threats.
- Includes logging, monitoring, encryption, firewalls, intrusion detection systems (IDS), and identification and authentication mechanisms.

Why is Access Control Important?

- **Protection of Sensitive Data:**
  Access control prevents unauthorized individuals from accessing confidential information, protecting intellectual property and confidential business data.
- **Prevention of Data Breaches:**
  By controlling access to systems and data, access control reduces the risk of data breaches and unauthorized access.
- **Compliance with Regulations:**
  Many industries have regulatory requirements for access control, ensuring compliance with standards like HIPAA (health data) and PCI DSS (financial data).
- **Security Posture Improvement:**
  Implementing robust access control policies significantly enhances overall security posture and reduces the organization's attack surface.

Why is Access Control Important?

- Victims of data compromises, with victim notices increasing by 312% from 419 million notices in 2023 to 1,728,519,397
- 74% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials, or social engineering
- In 2023 Infostealer activity increased by 266%
- The number of attacks featuring valid credentials saw a 71% increase year-over-year
- Out of the confirmed identity-based breaches that were identified within public domain 73% were the result of compromised credentials, and it’s estimated that the majority of the remaining 27% were the result of phishing attacks

Access Control From the State Perspective

- Organizations are required to implement necessary controls for providing authorized access and preventing unauthorized access to IT resources and information assets based on business and security requirements. All users of State and agency systems with access to non-public data must identify themselves and provide a means to authenticate their claimed identities appropriately for the risk level of the system and/or transaction.

- Access to State information technology assets shall be controlled and managed to ensure that only authorized devices/persons have appropriate access in accordance with an agency’s business needs.

- NIST has twenty-five (25) controls that are specific to Access Control and eleven (11) for Authentication

Access Control Key Concepts

Authentication:
Verifying the identity of a user or entity, typically through credentials like usernames and passwords, biometric scans, or security tokens.

Authorization:
Determining what specific permissions or access rights a user or entity has after being authenticated. This defines what they can access and do within the system.

Control Mechanisms:
The technical controls that enforce the policies and validate authentication and preform the authorization

Breaking Down Authentication and Authorization

Authentication		Authorization
Authentication is the process of verifying user identity before giving them permission to access a system, account, or file.	**Definition**	Authorization is the process of verifying a user's access level to a system, account, or file.
Its main purpose is to verify ("authenticate") a user's identity. It also keeps out suspicious or malicious users since their identities will not be verifiable.	**Purpose**	User authorization ensures that only authorized users can access the assets they need and only to the extent allowed by the system.
User authorization ensures that only authorized users can access the assets they need and only to the extent allowed by the system.	**Process**	Computer systems can leverage many types of authorization strategies, such as Role-Based Access Control (RBAC).
Credential-based authentication works by comparing user-provided credentials to a database record. When there is a perfect match between the two, users can access the account.	**Method**	Under RBAC, authorization permissions are associated with roles, not users. It ensures that users can only access the required information according to their roles.

from fortinet.com

Types of Access Control

- **Discretionary Access Control (DAC):**
  Allows users to grant or deny access to resources based on their own discretion. This can lead to inconsistencies and vulnerabilities if not carefully managed.
- **Mandatory Access Control (MAC):**
  Uses security labels and clearance levels to control access, based on predetermined policies. This can be more restrictive but provides a higher level of security.
- **Role-Based Access Control (RBAC):**
  Grants access based on a user's role within the organization, streamlining access management for similar roles.
- **Attribute-Based Access Control (ABAC):**
  Determines access based on a wider range of factors, including the user, resource, and environment.
- **Rule-Based Access Control (RuBAC):**
  Uses predefined rules to determine access, offering flexibility and control.

Access Control Fundamentals: Least Privilege

Least Privilege:
All users and processes should only be granted the minimum access or privileges that they need to perform their designated roles, or tasks and no more.

- **Attack Surface:** Limiting access reduces the number of potential points of entry for malicious actors.
- **Minimized Damage:** If an account is compromised, the harm is limited to the specific resources the user had access to.
- **Enhanced Operational Efficiency:** Systems accounts should be easier to manage provision, and operations streamlined by providing users with only the access they need.
- **Improved Security Posture:** Contributes to a more secure overall security posture through practices like isolation of critical subsystems and prevent non-privileged users from executing privileged functions.

Access Control Fundamentals: Revoking Access

Revoking access either individual or process at the right time, we can mitigate several risks associated with unauthorized access while simultaneously strengthening data governance. Remember strong access control cannot be on set-and-forget function and requires regular assessments and checks to prevent drift and unexpected data exposure.

Revocation of Access Right can be:

- Immediate or delayed
- Selective or general
- Partial or total i.e., all access rights or some
- Temporary or permanent

The same rules apply to both people a technology e.g., system accounts.

Access Control Fundamentals: Deprovisioning

While similar to revoking access, deprovisioning goes beyond merely removing access. It is a continuous process that requires precision, auditing, and constant monitoring to guarantee security and access quality.

Deprovisioning starts with the revocation of access

- **Deleting user credentials:** Usernames, passwords, and any other associated information that is part of the credentialling
- **Assessing and reviewing:** Rechecking deprovisioning steps to ensure they are successful i.e., user retains no access, and only appropriate credentials remain
- **Continuous monitoring:** Validation of access remains revoked and any unusual activities that could be security issues are identified
- **Documentation and logging:** Serves as a future point of reference, assist in regulatory compliance, and is a record of what was done

Access Control Best Practices

- Use Multifactor Authentication (MFA)where possible
- Enforce the use of strong password
- Do not share accounts
- Support the enablement of least privilege
- Control privileged access
- Identify and document the different types of account in use
- Work to ensure user account support is resilient to social engineering

Informational Slides

NC DHHS Privacy and Security Policies : https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security/

NC State Security Standards: https://it.nc.gov/programs/cybersecurity-risk-management/esrmo-initiatives/statewide-information-security-policies

The DHHS Privacy and Security Awareness Hub (Information and Training): https://www.ncdhhs.gov/about/administrative-offices/privacy-and-security/dhhs-privacy-and-security-awareness-hub

DIT Artificial Intelligence Resource Page: https://it.nc.gov/resources/artificial-intelligence

Next Meeting Planned for May 8, 2025

Questions