Control: 03.01.05 — Least Privilege

Assigned To:	Assigned By:	Date:

NIST 800-171 r3
03.01 Access Control

03.01.05 — Least Privilege

Overview
This control is about ensuring that users and system processes only have the access they need to perform their duties. It involves regularly reviewing and adjusting privileges, authorizing access to security functions and relevant information, and creating additional processes, roles, and system accounts as necessary.

Implementation Guidance
Start by defining the necessary security functions and relevant information for which access needs to be authorized. Then, establish a process for regularly reviewing and adjusting user privileges. Make sure to document all changes and keep a record of all authorizations.

Suggested Evidence
- Access control policies and procedures
- List of assigned access authorizations
- Records of privilege reviews and adjustments
- System configuration settings
- Audit records

Assessment Guidance
Documentation to Review
- access control policy and procedures
- procedures for least privilege
- list of assigned access authorizations (i.e., privileges)
- system configuration settings
- system audit records
- list of security functions (implemented in hardware, software, and firmware)
- security-relevant information for which access must be explicitly authorized
- list of system-generated roles or classes of users and assigned privileges
- validation reviews of privileges assigned to roles or classes of users
- records of privilege removals or reassignments for roles or classes of users

Personnel to Interview
- personnel with responsibilities for defining least privileges
- personnel with information security responsibilities
- system administrators

Mechanisms to Test
- mechanisms for implementing least privilege functions
- mechanisms for implementing reviews of user privileges

03.01.05 — Least Privilege

Official Description:
Organizations employ the principle of least privilege for specific duties and authorized access for users and system processes. Least privilege is applied to the development, implementation, and operation of the system. Organizations consider creating additional processes, roles, and system accounts to achieve least privilege. Security functions include establishing system accounts and assigning privileges, installing software, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information. Security-relevant information includes threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, security architecture, cryptographic key management information, access control lists, and audit information.

SR-03.01.05

- ☐ SR-03.01.05.a – a: Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.
- ☐ SR-03.01.05.b – b: Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].
- ☐ SR-03.01.05.c – c: Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.
- ☐ SR-03.01.05.d – d: Reassign or remove privileges, as necessary.

DS-A.03.01.05.a
system access for users (or processes acting on behalf of users) is authorized only when necessary to accomplish assigned organizational tasks.

DS-A.03.01.05.b[01]
access to <*A.03.01.05.ODP[01]: security functions*> is authorized.

➔ ***A.03.01.05.ODP[01]***
security functions for authorized access are defined.

DS-A.03.01.05.b[02]
access to <*A.03.01.05.ODP[02]: security-relevant information*> is authorized.

➔ ***A.03.01.05.ODP[02]***
security-relevant information for authorized access is defined.

DS-A.03.01.05.c
the privileges assigned to roles or classes of users are reviewed <*A.03.01.05.ODP[03]: frequency*> to validate the need for such privileges.

➔ ***A.03.01.05.ODP[03]***
the frequency at which to review the privileges assigned to roles or classes of users is defined.

DS-A.03.01.05.d
privileges are reassigned or removed, as necessary.

03.01.05 — Least Privilege

Is system access for users or processes authorized only when necessary to accomplish assigned tasks?

Is access to the defined security functions authorized?

- **What are the security functions for which access needs to be authorized?**
- ★ **Required**: at a minimum and if applicable: establishing system accounts and assigning privileges, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information.

Is system access for users or processes authorized only when necessary to accomplish assigned tasks?

- **What is the security-relevant information for which access needs to be authorized?**
- ★ **Required:** at a minimum and if applicable: threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, cryptographic key management information, security architecture, access control lists, and audit information

What is the defined frequency for reviewing privileges assigned to roles or classes of users?

- **How frequently should the privileges assigned to roles or classes of users be reviewed?**
- ★ **Required:** at least every 12 months

Are privileges reassigned or removed as necessary?

Evidence:

Control: 03.01.06 — Least Privilege – Privileged Accounts

Assigned To:	Assigned By:	Date: