[Insert Company Name Or Logo]	
Title: Least Privilege Protective Technology	**P&P #: [Insert Here]**
Approval Date: [Date]	**Review:**
Effective Date: [Date]	**Information Technology**

Purpose

This policy and procedure defines how to protect technology by ensuring the principle of "least privilege" is incorporated into organization operations. The policy gives the Security Officer and/or Information Security management personnel authority to implement rules that give users the least functionality to perform job duties, and to avoid potential security violations.

Scope

This policy applies to all employees and other members of the workforce (whether paid, contractor, or volunteer) working in all facilities under the organization's ownership and being granted access to any electronic information system.

Definitions

Least Privilege - The principle that a security architecture should be designed so that each entity and employee is granted the minimum system access, resources and authorizations that is needed to perform required functions.

Policy

The Security Officer will implement policies and procedures for ensuring users are only allowed to have the minimum roles to adequately complete their job duties. Security is top priority for the company, and it is the job of Security Officer to ensure that groups and individuals are not able to access or modify information that are not within the scope of their job description.

Procedures

The Security Officer and/or Information System Owner shall:

a) Update and maintain the policy document to reflect its current protective technology procedures and notify the appropriate individuals.
b) Ensure that all "least privilege" is implemented by adhering to the company's policies and procedures.

<u>The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</u>

1. The information security officers will take the following steps in ensuring least functionality is incorporated.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

a. Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
b. Configure information systems to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, and/or services that are not required for the business function of the information system.
c. Limit component functionality to a single function per device (e.g. database server, web server, etc.), where feasible.
d. Access to Company information systems is granted and managed by the user role and business function.
e. Disable any functions, ports, protocols, and services within an information system that are deemed to be unnecessary and/or non-secure.
f. Identify and remove/disable unauthorized and/or non-secure functions, ports, protocols, services, and applications.

Violations: Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or assignment, depending on the severity of the infraction.

Attachments: Security Incident Report Log

Related Policies:

Reference:
NIST SP 800-171 Revision 2, NIST Special Publication 800-53 Revision 5

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.