SI.L2-3.14.7

System & Information Integrity

Identify Unauthorized Use

"Identify unauthorized use of organizational systems."

Objectives

[a]
Authorized use of the system is defined.

[b]
Unauthorized use of the system is identified.

Key Discussion Points

Define Before You Detect:
[a] must precede [b] — without a defined baseline of authorized use, there is no standard against which to identify unauthorized activity.

Acceptable Use Policy:
The AUP is the primary vehicle for [a] — it must define authorized use by role, including what data can be accessed, from where, and by whom.

Audit Logs Are the Tool:
[b] is satisfied by reviewing audit logs for deviations from the authorized use baseline — IDS, SIEM, and user activity monitoring all support this.

Insider Threat Focus:
This control is particularly relevant to insider threat — authorized users who exceed their permitted access are the primary target of unauthorized use detection.

Assessment Methods

EXAMINE

System and information integrity policy; configuration management policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system configuration settings; scan results from malicious code protection mechanisms; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; personnel installing and maintaining the system; personnel with responsibility for malicious code protection.

TEST

Organizational processes for employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting malicious code protection including updates and configurations; mechanisms supporting malicious code scanning.

SI.L2-3.14.7

SYSTEM & INFO INTEGRITY — Identify Unauthorized Use

Plain English

What this control is really saying:

You cannot identify unauthorized use if you have not first defined what authorized use looks like. This control has a logical sequence: define what is permitted (acceptable use policy, role-based access), then use audit logs and monitoring tools to detect when something falls outside that definition. Both steps are required — [a] without [b] is documentation only; [b] without [a] has no baseline to compare against.

How it is used:

- An acceptable use policy defines authorized system use by role — standard users can access CUI files, admins can modify configurations, neither can access each other's functions.
- Audit logs from the CUI file server are reviewed weekly — access outside normal business hours, access to files outside a user's project assignment, and bulk downloads all generate alerts.
- User activity monitoring software detects when a user accesses sensitive directories not associated with their current work — an alert is generated and the access is investigated.
- IDS rules flag connections from CUI workstations to known-bad domains — the activity is cross-referenced against authorized user activity to determine if a session is legitimate.

Real World Example

The Scenario

Acme Defense has an acceptable use policy that prohibits personal use of CUI systems. Audit logging is enabled but logs are never reviewed. No tools are in place to detect policy violations or unauthorized access.

What the assessor finds

A disgruntled employee with a pending termination spends two weeks copying CUI design files to a personal USB drive. The access was logged. Nobody reviewed the logs. The unauthorized copying was discovered six months later when the employee's new employer used the designs in a competing proposal.

SPRS Score Impact

3.14.7 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

Authorized use defined in acceptable use policy by role, audit logs reviewed on defined schedule, monitoring tools configured to flag deviations from authorized use baseline, unauthorized access events investigated and documented.

Common Gaps

What assessors actually find in the field:

✗ **Authorized use not defined**

No acceptable use policy defines what users are permitted to do — [b] cannot be met because there is no baseline to compare observed activity against.

✗ **Logs not monitored**

Audit logs exist but are never reviewed — unauthorized access events are recorded but not detected.

✗ **No role-based use definition**

Authorized use is defined for 'users' generically — no role-specific definitions exist for administrators, technicians, or contractors.

✗ **Former employee access not caught**

A terminated employee's account was not disabled — they accessed CUI files for three weeks post-termination and the access was not detected.

✗ **Anomalous access no baseline**

The organization attempts to detect unusual access but has no documented baseline of normal activity — every review is qualitative judgment with no standard.