**Prevention Patterns –**

**Security Requirements Patterns related to Preventing Security Breaches**

# **P-C\_I\_PR-1**

* *Name\**: P-C\_I\_PR-1: Prevent unauthorized access to information.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Privacy> of information.
* *Context\**: All access to information should be in accordance with an access control / privacy policy and applicable regulations.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Information
* *Solution\**: The system shall:

1. enforce that all access to <information | system> are in accordance with <applicable access control policies | access control decisions>.
2. enforce that flow of information <within the system | between systems> is in accordance with applicable <information flow policies | access restrictions>.
3. <handle | retain> information <within | output from> the system in accordance with <applicable laws | policies | standards | regulations | operational requirements>.
4. protect the <confidentiality | integrity | privacy> of information <at rest | in use | in transmission>.
5. have provision to <establish | assign | retain> security attributes for information <at rest | in use | in transmission>.

* *Source\**: AC-3, AC-4, AC-16, AC-21, AC-24, SC-16, SC-8, SC-28, SI-12.
* *See Also\**: P-C\_I\_PR-2: Limit authorized access to information, P-C\_I\_PR-3: Restrict access to media, P-C\_PR-1: Prevent information leakage, P-ID-1: Identify and authenticate system users, P-AY-1: Enable auditing of events, D-C\_PR-1: Detect unauthorized disclosure of information, R-C\_PR-1: Respond to unauthorized disclosure of information.

# **P-C\_I\_PR-2**

* *Name\**: P-C\_I\_PR-2: Limit authorized access to information.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Privacy> of information.
* *Context\**: All access to information should be limited to only necessary accesses required to perform the authorized tasks.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Information
* *Solution\**: The organization shall:

1. define access authorizations to support separation of duties of <users | processes acting on behalf of users> to reduce the risk of abusing authorized privileges.
2. employ least privilege, allowing only authorized accesses for <users | processes acting on behalf of users> which are necessary to accomplish assigned tasks.

* *Source\**: AC-5, AC-6.
* *See Also\**: P-C\_I\_PR-1: Prevent unauthorized access to information, P-C\_PR-1: Prevent information leakage, P-ID-1: Identify and authenticate system users, P-AY-1: Enable auditing of events, D-C\_PR-1: Detect unauthorized disclosure of information, R-C\_PR-1: Respond to unauthorized disclosure of information, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity.

# **P-C\_I\_PR-3**

* *Name\**: P-C\_I\_PR-3: Restrict access to media.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Privacy> of media containing information.
* *Context\**: The types of media used in the system and types of access to the media containing information should be in accordance with the necessary authorizations.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Information
* *Solution\**: The organization shall:

1. restrict access to <digital | non-digital> media to <authorized users | authorized locations | authorized transfers outside the organization>.
2. protect the <digital | non-digital> medial until the media are <destroyed | adequately sanitized | appropriately downgraded>.
3. maintain <confidentiality | integrity | privacy | accountability> of <digital | non-digital> media during <transfer> outside of controlled areas.
4. <restrict | prohibit> the usage of <certain type of media> on <specific system components>.

* *Source\**: MP-2, MP-4, MP-5, MP-6, MP-7, MP-8.
* *See Also\**: P-C\_I\_PR-1: Prevent unauthorized access to information, P-C\_I\_PR-2: Limit authorized access to information, P-C\_PR-1: Prevent information leakage, P-AY-1: Enable auditing of events, D-C\_PR-1: Detect unauthorized disclosure of information, R-C\_PR-1: Respond to unauthorized disclosure of information.

# **P-C\_PR-1**

* *Name\**: P-C\_PR-1: Prevent information leakage.
* *Problem\**: <prevent> a breach of <Confidentiality | Privacy> of information.
* *Context\**: The system shall prevent unintended disclosure of information that is not in accordance with an access control / privacy policy and applicable regulations.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Information
* *Solution\**: The system shall:

1. prevent <unauthorized | unintended> information transfer via shared <internal | external> resources (e.g., registers, memory, disks).
2. validate information output from <defined programs | applications> to ensure consistency with expected content so that information is only disclosed as <authorized | intended>.
3. protect against information disclosure during <error handling | authentication> by revealing feedback <without revealing information that could be exploited | only to authorized personnel>.

* *Source\**: SC-4, SI-11, SI-15, IA-6.
* *See Also\**: P-C\_I\_PR-1: Prevent unauthorized access to information, P-C\_I\_PR-3: Restrict access to media, P-ALL-1: Enable continuous monitoring, D-C\_PR-1: Detect unauthorized disclosure of information, R-C\_PR-1: Respond to unauthorized disclosure of information.

# **P-C\_PR-2**

* *Name\**: P-C\_PR-2: Prevent unauthorized remote sensing and activation.
* *Problem\**: <prevent> a breach of <Confidentiality | Privacy> of information accessed through remote sensors.
* *Context\**: The system allows remote activation of sensors and devices only in exceptional, pre-defined situations.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Communication
* Type of communication channel: Remote
* *Solution\**: The system shall:

1. prohibit remote activation of <environmental sensing capabilities | collaborative computing devices> other than <defined exceptions>.
2. provide explicit indication when <sensor | device> is in use to <authorized user>.

* *Source\**: SC-15, SC-42.
* *See Also\**: P-C\_I\_PR-1: Prevent unauthorized access to information, P-C\_PR-1: Prevent information leakage, P-CIA\_PR-1: Manage secure internal and external connections, P-ID-1: Identify and authenticate system users, P-AY-1: Enable auditing of events, D-ID-1: Detect malicious activity during authentication.

# **P-AY-1**

* *Name\**: P-AY-1: Enable auditing of events.
* *Problem\**: <prevent> a breach of <Accountability>.
* *Context\**: The organization wants to have capability to perform audits in accordance with audit and accountability policy and procedures.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The organization shall:

1. identify auditable events that can support after-the-fact investigation of security incidents.
2. define <frequency | conditions> under which the <auditable events> should be <recorded | reviewed>.
3. allocate sufficient audit storage capacity in accordance with <defined audit storage requirements> to avoid <loss of audit records | limitation of audit capability>.
4. define methods for coordinating <audit information> when <audit information> is transmitted across organization boundaries.

* *Source\**: AU-2, AU-4, AU-16.
* *See Also\**: P-AY-2: Generate audit records and reports, P-AY-3: Protect confidentiality and integrity of audit records, P-ID-1: Identify and authenticate system users, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity.

# **P-AY-2**

* *Name\**: P-AY-2: Generate audit records and reports.
* *Problem\**: <prevent> a breach of <Accountability>.
* *Context\**: The system shall generate audit records and reports to support accountability and non-repudiation.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The system shall:

1. generate audit records containing necessary information including type, time, location, source and outcome of the <auditable event> and identity of <individuals | subjects> associated with the <auditable event>.
2. use internal system clocks to generate and record timestamps for <auditable events> at <specified granularity>.
3. provide <on-demand | after-the-fact> audit report generation capability.
4. protect against <user> denying having performed <defined actions>.

* *Source\**: AU-3, AU-7, AU-8, AU-10.
* *See Also\**: P-AY-1: Enable auditing of events, P-AY-3: Protect confidentiality and integrity of audit records, P-ID-1: Identify and authenticate system users, D-ALL-2: Analyze audit records to detect malicious activity.

# **P-AY-3**

* *Name\**: P-AY-3: Protect confidentiality and integrity of audit records.
* *Problem\**: <prevent> a breach of <Accountability>.
* *Context\**: The system shall protect the confidentiality and integrity of audit records and any reports generated from the records.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Security / Information
* *Solution\**: The system shall:

1. prevent alteration of the original content and ordering of <audit records>.
2. protect audit <information | tools> from unauthorized <access | modification | deletion>.

* *Source\**: AU-7, AU-9.
* *See Also\**: P-AY-1: Enable auditing of events, P-AY-2: Generate audit records and reports, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-AY-1: Respond to failures in accountability.

# **P-I-1**

* *Name\**: P-I-1: Protect system integrity at runtime.
* *Problem\**: <prevent> a breach of <Integrity> of the system functions.
* *Context\**: The integrity of system functionality should be maintained during execution.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**:

1. The system shall implement a reference monitor to enforce <defined access control policies> that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.
2. The system shall have provision to load and execute <define components | defined applications> from hardware-enforced, read-only media.
3. The system shall maintain a separate execution domain for each executing process.
4. The system shall check the validity of the <syntax | semantics> of the information input to the system.
5. The organization shall employ <isolated execution environment | virtualized sandbox> for <defined systems | defined components | defined locations> to <quickly identify malicious code | reduce likelihood of malicious code propagation>.

* *Source\**: AC-25, SC-34, SC-39, SC-44, SI-10, SI-16.
* *See Also\**: P-C\_PR-1: Prevent information leakage, P-I\_A-1: Limit unnecessary exposure of system functionality, P-ALL-1: Enable continuous monitoring, P-ID-2: Establish authenticity of system components, P-ALL-2: Limit system exposure to persistent attackers, P-ALL-3: Deceive persistent attackers, D-I-1: Detect malicious system modification attempts, D-I-2: Detect vulnerabilities in the system, R-I-1: Respond to vulnerabilities in the system.

# **P-I\_A-1**

* *Name\**: P-I\_A-1: Limit unnecessary exposure of system functionality.
* *Problem\**: <prevent | respond to> a breach of <Integrity | Availability> of the system functions.
* *Context\**: The integrity of system functionality should be maintained by limiting unnecessary exposure.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The organization shall:

1. <physically | logically> separate user functionality from information system management functionality.
2. employ <diverse set of technologies | physical distribution of processing and storage | logical separation of processing and storage> so that an attack on one part of the system does not affect other parts of the system.
3. isolate security functions from non-security functions.
4. physically partition <defined components> based on <defined circumstances>.
5. physically <disable | remove> <defined connection ports | input devices> on <defined components>.

* *Source\**: SC-2, SC-3, SC-29, SC-32, SC-36, SC-41.
* *See Also\**: P-C\_PR-1: Prevent information leakage, P-I-1: Protect system integrity at runtime, P-ALL-2: Limit system exposure to persistent attackers, P-ALL-3: Deceive persistent attackers, D-I-3: Detect problems with security functions.

# **P-ID-1**

* *Name\**: P-ID-1: Identify and authenticate system users.
* *Problem\**: <prevent> a breach of <Identification and authentication> of the system users.
* *Context\**: The identity and authenticity of system users should be established and maintained through each user session.
* Type of the pattern\*: Technical
* Scope of the pattern\*: User
* *Solution\**: The system shall:

1. uniquely identify and authenticate <organizational | non-organizational> <users | processes acting on behalf of users | services | devices> before allowing access to the system <locally | via a network>.
2. allow access to the system only after <establishing | re-establishing> identification and authentication procedures.
3. explicitly specify and document rationale for <defined actions> that are allowed without identification or authentication.
4. limit the number of concurrent sessions for <user account type> to <defined limit>.
5. prevent access to the system by <locking | terminating> the session <at user's request | after defined inactive period>.

* *Source\**: IA-2, IA-3, IA-8, IA-9, AC-10, AC-11, AC-14.
* *See Also\**: P-AY-1: Enable auditing of events, P-C\_PR-1: Prevent information leakage, P-C\_I\_ID-1: Manage security of identifiers and authenticators, P-C\_I\_ID-2: Manage security of cryptographic functions, P-C\_I\_ID-3: Manage security of communication session, D-ID-1: Detect malicious activity during authentication, R-ID-1: Respond to malicious activity during authentication.

# **P-ID-2**

* *Name\**: P-ID-2: Establish authenticity of system components.
* *Problem\**: <prevent> a breach of <Identification and authentication> of the system components.
* *Context\**: The authenticity of system components should be established.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The organization shall:

1. detect and prevent counterfeit components from entering the system based on <defined anti-counterfeit policy and procedures>.
2. report counterfeit components to <source of the counterfeit component | authorized organizations | authorized personnel>.

* *Source\**: SA-19.
* *See Also\**: P-AY-1: Enable auditing of events, P-I-1: Protect system integrity at runtime, D-I-1: Detect malicious system modification attempts.

# **P-C\_I\_ID-1**

* *Name\**: P-C\_I\_ID-1: Manage security of identifiers and authenticators.
* *Problem\**: <prevent> a breach of < Confidentiality | Integrity | Identification & Authentication> during authentication.
* *Context\**: The organization uses identifiers and authenticators to establish identity and authorization for the security of the system. The security of the identifiers and authenticators themselves must be protected.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Security
* *Solution\**: The system shall:

1. assign unique identifiers for <individuals | groups | roles | services | devices> only after receiving necessary authorizations.
2. prevent the reuse of identifiers for <defined time period>.
3. disable identifiers <after defined inactive period>.
4. verify identity of <individual | group | role | service | device> before initially distributing the authenticator.
5. <establish | implement> procedures for <initial authenticator distribution | updating the authenticator | a lost or compromised authenticator | a damaged authenticator | revoking authenticators>.
6. establish <initial content | lifetime restrictions | reuse conditions> for authenticators.
7. protect authenticator content from unauthorized <disclosure | modification>.
8. change authenticators in the event of <system installation | change in group membership | change of role | expiration based on defined time>.

* *Source\**: IA-4, IA-5.
* *See Also\**: P-ID-1: Identify and authenticate system users, P-C\_PR-1: Prevent information leakage, D-ID-1: Detect malicious activity during authentication, R-ID-1: Respond to malicious activity during authentication, P-C\_I\_ID-2: Manage security of cryptographic functions, R-SEC-1: Respond to threats to security functions.

# **P-C\_I\_ID-2**

* *Name\**: P-C\_I\_ID-2: Manage security of cryptographic functions.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Identification & Authentication> of cryptographic functions.
* *Context\**: The organization uses cryptographic functions for confidentiality and integrity of information. The security of the cryptographic functions themselves must be protected.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Security
* *Solution\**: The organization:

1. <establishes | manages | implements> cryptographic functions in accordance with <applicable laws | regulations | policies | standards>.
2. implements mechanism for authentication to cryptographic modules that meet the requirements of <applicable laws | regulations | policies | standards>.
3. issues public key certificates in accordance with <a defined certificate policy>
4. obtains certificates from <an approved service provider>.

* *Source\**: SC-12, SC-13, SC-17, IA-7.
* *See Also\**: P-C\_I\_ID-1: Manage security of identifiers and authenticators, P-C\_PR-1: Prevent information leakage, R-SEC-1: Respond to threats to security functions.

# **P-C\_I\_ID-3**

* *Name\**: P-C\_I\_ID-3: Manage security of communication session.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Identification & Authentication> of communication sessions.
* *Context\**: The organization allows communication sessions over a network. The security of the established communication sessions themselves must be protected.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Security / Communication
* Type of communication channel: Local, Network, Wireless.
* *Solution\**: The system shall:

1. establish a trusted communications path with the user for <authentication | re-authentication | other security functions>.
2. terminate network connections associated with a communications session <at session end | after defined inactive period>.
3. protect the authenticity of communications sessions.

* *Source\**: SC-10, SC-11, SC-23.
* *See Also\**: P-ID-1: Identify and authenticate system users, P-C\_PR-1: Prevent information leakage, P-I\_A\_ID-1: Setup secure name and address resolution functions, P-CIA\_PR-1: Manage secure internal and external connections.

# **P-CIA\_PR-1**

* *Name\**: P-CIA\_PR-1: Manage secure internal and external connections.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Availability | Privacy> when establishing connections.
* *Context\**: The organization allows connections with components, devices, networks and systems internal or external to the organization.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Communication
* Type of communication channel: Local, Network, Wireless
* *Solution\**: The organization shall:

1. authorize internal connections with <defined component classes (e.g., printers, scanners, mobile devices)>.
2. document <interface characteristics | security requirements | nature of information communicated> for each internal connection with the <defined component class>.
3. allow connection to external networks only through managed interfaces (e.g., gateways, routers, firewalls, encrypted tunnels) in accordance with <organizational security architecture>.
4. monitor and control communication at the <external boundary | key internal boundaries> of the system.
5. implement subnetworks for publicly accessible system components that are <logically | physically> separated from internal organizational networks.
6. protect <external | internal> <defined wireless links> from <information disclosure | denial of service | spoofing | defined types of attacks>.

* *Source\**: CA-9, SC-7, SC-40.
* *See Also\**: P-C\_I\_PR-1: Prevent unauthorized access to information, P-C\_PR-1: Prevent information leakage, P-C\_PR-2: Prevent unauthorized remote sensing and activation, P-C\_I\_ID-2: Manage security of cryptographic functions, P-C\_I\_ID-3: Manage security of communication session.

# **P-I\_A\_ID-1**

* *Name\**: P-I\_A\_ID-1: Setup secure name and address resolution functions.
* *Problem\**: <prevent> a breach of < Integrity | Availability | Identification & Authentication> when establishing communication.
* *Context\**: The system shall be able to verify integrity and authenticity of the source of information across a network.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Communication
* Type of communication channel: Local network, remote network, wireless network.
* *Solution\**: The system shall:

1. have provision that the <name | address> resolution services employ separate servers for internal and external roles.
2. implement any <name | address> resolution services in a fault-tolerant manner by employing <redundancy | geographical distribution>.
3. perform <data origin authentication | data integrity verification> for <name | address> resolution services provided by <external authoritative source | recursive resolvers | caching resolvers>.
4. enable verification of <child zones | chain of trust among parent and child domains> for <distributed | hierarchical> namespaces.

* *Source\**: SC-20, SC-21, SC-22.
* *See Also\**: P-C\_I\_ID-3: Manage security of communication session, P-CIA\_PR-1: Manage secure internal and external connections, D-ID-1: Detect malicious activity during authentication, R-ID-1: Respond to malicious activity during authentication.

# **P-ALL-1**

* *Name\**: P-ALL-1: Enable continuous monitoring.
* *Problem\**: <prevent | detect | respond to> a breach of < Confidentiality | Integrity | Availability | Identification & Authentication | Accountability | Privacy>.
* *Context\**: The organization shall enable continuous monitoring of events.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The organization shall:

1. <develop | implement> a continuous monitoring strategy.
2. define <metrics> to be monitored and <frequency> for <monitoring | security control assessments>.
3. perform <security control assessments | security status monitoring of defined metrics> in accordance with the continuous monitoring strategy.
4. correlate information from <monitoring | assessment> activities and take appropriate response actions.

* *Source\**: CA-7.
* *See Also\**: P-I-1: Protect system integrity at runtime, P-AY-1: Enable auditing of events, D-I-1: Detect malicious system modification attempts, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-CIA-1: Respond to system failure conditions, R-AY-1: Respond to failures in accountability, R-SEC-1: Respond to threats to security functions.

# **P-ALL-2**

* *Name\**: P-ALL-2: Limit system exposure to persistent attackers.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Availability | Identification & Authentication | Accountability | Privacy> of the system.
* *Context\**: Advanced persistent threats (APTs), e.g., attackers who persists in their attempts to gain unauthorized access to the system, exist. Limiting the system functionality available to the attackers may safeguard the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* Type of threat: Advanced persistent threat
* *Solution\**: The organization may:

1. employ <defined components> with minimal <functionality | information storage>.
2. may implement non-persistent <defined components | defined services> that are initiated in a known state and terminated <upon end of session | periodically at defined frequency> to limit opportunity for attack.

* *Source\**: SC-25, SI-14.
* *See Also\**: P-C\_PR-1: Prevent information leakage, P-I\_A-1: Limit unnecessary exposure of system functionality, P-ALL-1: Enable continuous monitoring, P-ALL-3: Deceive persistent attackers, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-CIA-1: Respond to system failure conditions, R-SEC-1: Respond to threats to security functions.

# **P-ALL-3**

* *Name\**: P-ALL-3: Deceive persistent attackers.
* *Problem\**: <prevent> a breach of <Confidentiality | Integrity | Availability | Identification & Authentication | Accountability | Privacy> of the system.
* *Context\**: Advanced persistent threats (APTs), e.g., attackers who persists in their attempts to gain unauthorized access to the system, exist. Deceiving the attackers may provide valuable time to safeguard the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* Type of threat: Advanced persistent threat
* *Solution\**: The organization may:

1. setup easier targets for the attackers such as <honeypots | others>.
2. employ tactics such as <randomness | uncertainty | virtualization > to confuse and mislead the attackers.

* *Source\**: SC-26, SC-30.
* *See Also\**: P-C\_PR-1: Prevent information leakage, P-ALL-1: Enable continuous monitoring, P-ALL-2: Limit system exposure to persistent attackers, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-CIA-1: Respond to system failure conditions, R-SEC-1: Respond to threats to security functions.

**Detection Patterns –**

**Security Requirements Patterns related to Detecting Security Breaches**

# **D-C\_PR-1**

* *Name\**: D-C\_PR-1: Detect unauthorized disclosure of information.
* *Problem\**: <detect> a breach of <Confidentiality | Privacy> of information.
* *Context\**: All disclosures of information should be in accordance with an access control / privacy policy and applicable regulations. Any disclosure not in accordance with the policy should be detected.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Information
* *Solution\**: The system shall detect unauthorized disclosures of <resource> through:

1. monitoring the status and location of system components that <store> unencrypted <resource>.
2. monitoring when <resource> leaves the secure system boundary during <storage | transfer>.
3. detecting malicious attempts at gaining access to information during <transfer> by exploiting the <transmission protocols>.
4. protecting against and detecting unauthorized mining of <resource> during <read | store | transfer>
5. performing analysis of potential covert channels that can be used to <read | transfer> the <resource>.

* *Source\**: AU-13, SC-31, AC-23, SC-19.
* *See Also\**: P-C\_I\_PR-1: Prevent unauthorized access to information, P-C\_I\_PR-2: Limit authorized access to information, P-C\_I\_PR-3: Restrict access to media, P-C\_PR-1: Prevent information leakage, R-C\_PR-1: Respond to unauthorized disclosure of information, P-ALL-1: Enable continuous monitoring, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity.

# **D-ID-1**

* *Name\**: D-ID-1: Detect malicious activity during authentication.
* *Problem\**: <detect> a breach of <Identification & Authentication> of the user.
* *Context\**: An attacker may try to authenticate as a regular user and gain unauthorized access to the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: User
* *Solution\**: The system shall maintain a record of:

1. unsuccessful logon attempts by <user>.
2. previous logon <time | location> that the <user> accessed the <resource> to <detect | alert authorized user about> suspicious activity.
3. frequent <location | device> from where the <user> accesses the system to <detect | alert authorized user about> deviations from the norm that may indicate potentially malicious activity.

* *Source\**: AC-7, AC-9.
* *See Also\**: P-ID-1: Identify and authenticate system users, P-C\_I\_ID-1: Manage security of identifiers and authenticators, R-ID-1: Respond to malicious activity during authentication, P-ALL-1: Enable continuous monitoring, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity.

# **D-I-1**

* *Name\**: D-I-1: Detect malicious system modification attempts.
* *Problem\**: <detect> a breach of <Integrity> of the system.
* *Context\**: An attacker may try to modify parts of the system functionality to gain unauthorized access to the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The organization shall:

1. detect if a code is untrusted or malicious through <vulnerability scanning | tamper resistance and detection | spam protection>.
2. monitor and maintain record of any <local | remote> maintenance activities performed on the system.
3. monitor and maintain record of any <local | remote> tools used for maintenance.
4. check for <integrity | authenticity> of <external components> that are included as part of the system.

* *Source\**: SA-18, SA-19, SC-18, SI-3, SI-7, SI-8, MA-2, MA-3, MA-4.
* *See Also\**: P-I-1: Protect system integrity at runtime, P-ID-2: Establish authenticity of system components, D-I-2: Detect vulnerabilities in the system, D-I-3: Detect problems with security functions, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity.

# **D-I-2**

* *Name\**: D-I-2: Detect vulnerabilities in the system.
* *Problem\**: <prevent | detect | respond to> a breach of <Integrity> of the system.
* *Context\**: The system may contain vulnerabilities that an attacker can exploit to gain unauthorized access to the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The system shall:

1. scan for vulnerabilities in <platforms | software | configurations> using <defined vulnerability scanning tools | defined techniques>.
2. conduct the vulnerability scans <periodically | as new vulnerabilities become known>.

* *Source\**: RA-5.
* *See Also\**: P-I-1: Protect system integrity at runtime, P-I\_A-1: Limit unnecessary exposure of system functionality, P-C\_I\_ID-1: Manage security of identifiers and authenticators, R-I-1: Respond to vulnerabilities in the system, P-ALL-1: Enable continuous monitoring, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity.

# **D-I-3**

* *Name\**: D-I-3: Detect problems with security functions.
* *Problem\**: <detect> a breach of <Integrity> of the security functions.
* *Context\**: An attacker may try to compromise or bypass the security mechanisms themselves to gain unauthorized access to the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Security
* *Solution\**: The system shall

1. verify integrity of security functions and notify <authorized individual> if any problems are identified.
2. record any <local | remote> maintenance activities performed on the system or any tools used for maintenance.

* *Source\**: SI-6.
* *See Also\**: P-I\_A-1: Limit unnecessary exposure of system functionality, D-I-1: Detect malicious system modification attempts, P-C\_I\_ID-1: Manage security of identifiers and authenticators, P-ALL-1: Enable continuous monitoring, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity.

# **D-ALL-1**

* *Name\**: D-ALL-1: Monitor for security incidents.
* *Problem\**: <detect > a breach of <Confidentiality | Integrity | Availability | Identification & Authentication | Accountability | Privacy> of the system.
* *Context\**: Security incidents, such as intrusion or unauthorized access to the system, should not go unnoticed.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The system shall:

1. setup mechanisms for monitoring security incidents related to <potential attacks | unauthorized connections> for <resource>.
2. have provisions to heighten the level of <monitoring activities> if an attack is detected or perceived.
3. setup notifications about the usage of system to detect <unauthorized access> of <resource>.
4. protect the <confidentiality | integrity> of information obtained from the intrusion monitoring tools.

* *Source\**: IR-4, IR-5, IR-6, SI-4, AC-8.
* *See Also\**: P-ALL-1: Enable continuous monitoring, D-I-1: Detect malicious system modification attempts, D-ALL-2: Analyze audit records to detect malicious activity, R-CIA-1: Respond to system failure conditions, R-AY-1: Respond to failures in accountability.

# **D-ALL-2**

* *Name\**: D-ALL-2: Analyze audit records to detect malicious activity.
* *Problem\**: <detect > a breach of <Confidentiality | Integrity | Availability | Identification & Authentication | Accountability | Privacy> of the system.
* *Context\**: Regular audits can help uncover malicious activity in the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The system shall:

1. setup mechanisms for <review | analysis | reporting> of audit records related to <system access | maintenance>.
2. retain audit records for <resource> for a <designated period> in accordance with applicable <policy | law>.
3. have mechanisms to generate activity for <resource> based on audit records.
4. provide <authorized users> with ability to <capture | record | view | hear> <user session>.

* *Source\**: AU-6, AU-11, AU-12, AU-14.
* *See Also\**: P-AY-1: Enable auditing of events, P-AY-2: Generate audit records and reports, P-AY-3: Protect confidentiality and integrity of audit records, D-C\_PR-1: Detect unauthorized disclosure of information, D-ID-1: Detect malicious activity during authentication, D-ALL-1: Monitor for security incidents, R-AY-1: Respond to failures in accountability.

**Response Patterns –**

**Security Requirements Patterns related to Responding to Security Breaches**

# **R-C\_PR-1**

* *Name\**: R-C\_PR-1: Respond to unauthorized disclosure of information.
* *Problem\**: <respond to> a breach of <Confidentiality | Privacy> of information.
* *Context\**: In case of unauthorized disclosure of information, the organization shall take appropriate remedial actions in accordance with the appropriate policies and regulations.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Information
* *Solution\**: The system shall:

1. respond to information spillage related to <resource> by <notifying authorize user | isolating compromised components | removing information from the compromised components>.
2. proactively assess if any additional components may have been compromised by the information spillage related to <resource>.

* *Source\**: IR-9.
* *See Also\**: P-ALL-2: Limit system exposure to persistent attackers, P-C\_I\_PR-1: Prevent unauthorized access to information, D-C\_PR-1: Detect unauthorized disclosure of information, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-CIA-1: Respond to system failure conditions.

# **R-ID-1**

* *Name\**: R-ID-1: Respond to malicious activity during authentication.
* *Problem\**: <prevent | respond to> a breach of <Identification & Authentication>.
* *Context\**: An attacker may try to pose as a regular user and gain unauthorized access to the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: User
* *Solution\**: The system shall:

1. have provision to lock the <local | remote> session of <user> if a breach of security is detected.
2. have provision to terminate the <local | remote> session of <user> if a breach of security is detected.
3. have provision to request additional authentication from <user> if a potential threat is detected.
4. require <user> to re-authenticate if a potential threat is detected.

* *Source\**: AC-11, AC-12, IA-10, IA-11.
* *See Also\**: P-ID-1: Identify and authenticate system users, P-C\_I\_ID-1: Manage security of identifiers and authenticators, D-ID-1: Detect malicious activity during authentication, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-CIA-1: Respond to system failure conditions, P-ALL-2: Limit system exposure to persistent attackers.

# **R-I-1**

* *Name\**: R-I-1: Respond to vulnerabilities in the system.
* *Problem\**: <respond to> a breach of <Integrity> of the system.
* *Context\**: The system may contain vulnerabilities that can be exploited by an attacker.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The system shall:

1. analyze vulnerabilities detected in <platforms | software | configurations> for potential harmful impact.
2. take steps to remediate legitimate vulnerabilities in <the given system | other information systems with potentially similar vulnerabilities>.

* *Source\**: RA-5.
* *See Also\**: P-I-1: Protect system integrity at runtime, P-I\_A-1: Limit unnecessary exposure of system functionality, D-I-2: Detect vulnerabilities in the system, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, P-ALL-2: Limit system exposure to persistent attackers.

# **R-A-1**

* *Name\**: R-A-1: Setup backup and recovery procedures.
* *Problem\**: <prevent | respond to> a breach of <Availability> of information assets.
* *Context\**: An attacker may compromise the system and render the information assets unavailable.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Information
* *Solution\**: The system shall:

1. conduct regular backup of <user | system | security> information.
2. have provision to protect the <confidentiality | integrity> of backup information similar to the original information.
3. be able to recover from backups of <user | system | security> information.

* *Source\**: CP-9, CP-10.
* *See Also\**: P-C\_I\_PR-1: Prevent unauthorized access to information, D-C\_PR-1: Detect unauthorized disclosure of information, R-A-2: Prevent and respond to denial of service, R-AY-1: Respond to failures in accountability, R-CIA-1: Respond to system failure conditions.

# **R-A-2**

* *Name\**: R-A-2: Prevent and respond to denial of service.
* *Problem\**: <prevent | respond to> a breach of <Availability> of the system.
* *Context\**: An attacker may compromise the system and render parts of the information system unavailable.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The system shall:

1. <protect against | limit> the effects of the denial of service attacks on <system components>.
2. <protect | limit> the availability of shared resources by allocating <defined resources> based on <priority | quota> of requesting <processes | users>.
3. include platform-independent applications for <organization-defined functions> to <promote portability | increase availability> in case a specific platform is under attack.

* *Source\**: SC-5, SC-6, SC-27.
* *See Also\**: P-ALL-1: Enable continuous monitoring, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-ALL-1: Respond to security incidents in the system, R-CIA-1: Respond to system failure conditions.

# **R-AY-1**

* *Name\**: R-AY-1: Respond to failures in accountability.
* *Problem\**: <respond to> a breach of <Accountability> of user actions.
* *Context\**: An attacker may compromise the mechanisms for accountability to covertly perform malicious activity in the system.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Security
* *Solution\**: The system shall:

1. respond to audit processing failures by alerting <authorized user>.
2. provision for alternate audit capability to record <designated actions> if the primary audit capability fails.

* *Source\**: AU-5, AU-15.
* *See Also\**: P-ALL-1: Enable continuous monitoring, P-ALL-2: Limit system exposure to persistent attackers, D-ALL-1: Monitor for security incidents, D-ALL-2: Analyze audit records to detect malicious activity, R-ALL-1: Respond to security incidents in the system, R-A-1: Setup backup and recovery procedures.

# **R-CIA-1**

* *Name\**: R-CIA-1: Respond to system failure conditions.
* *Problem\**: <prevent | respond to> a breach of <Confidentiality | Integrity | Availability> of the system.
* *Context\**: The system should respond to failure conditions such that security of the system is not further compromised beyond the current breach.
* Type of the pattern\*: Technical
* Scope of the pattern\*: System
* *Solution\**: The system shall:

1. have provision to switch operations to safe mode when <organization defined conditions> are detected.
2. fail in a known state in response to <security attacks> to help prevent further loss to security of the system.
3. proactively provide alternate <system components> in case of predictable failures (e.g., based on mean time to failure).
4. implement fail-safe procedures such as <alerting authorized personnel | reestablish system settings | shut down | restart > when <predefined failure conditions> occur.

* *Source\**: CP-12, SC-24, SI-13, SI-17.
* *See Also\**: P-ALL-1: Enable continuous monitoring, P-ALL-2: Limit system exposure to persistent attackers, P-ALL-3: Deceive persistent attackers, D-ALL-1: Monitor for security incidents, R-A-1: Setup backup and recovery procedures, R-A-2: Prevent and respond to denial of service, R-AY-1: Respond to failures in accountability.

# **R-SEC-1**

* *Name\**: R-SEC-1: Respond to threats to security functions.
* *Problem\**: <respond to> a breach of <Confidentiality | Integrity | Availability | Identification & Authentication | Accountability | Privacy> of the security functions.
* *Context\**: The system should handle situations in which the security functions and mechanisms may themselves be compromised.
* Type of the pattern\*: Technical
* Scope of the pattern\*: Security
* *Solution\**: The system:

1. may provide alternate <security mechanisms> in case a threat to <security mechanism> is detected (e.g., biometrics, temporary passwords, alternate communication protocols).
2. may employ separate communication channels to share security sensitive information including <identifiers | configuration information | cryptographic keys | security updates | system backups>.
3. shall have provision to <shut down | restart | other actions> the system when anomalies are discovered during security functions verification.

* *Source\**: CP-11, CP-13, SC-37, SI-6.
* *See Also\**: P-C\_I\_ID-1: Manage security of identifiers and authenticators, P-C\_I\_ID-2: Manage security of cryptographic functions, P-C\_I\_ID-3: Manage security of communication session, P-ALL-1: Enable continuous monitoring, P-ALL-2: Limit system exposure to persistent attackers, P-ALL-3: Deceive persistent attackers, D-ALL-1: Monitor for security incidents, R-CIA-1: Respond to system failure conditions, R-AY-1: Respond to failures in accountability.