Privileged Access Management Policy in SCADA Systems

VoltCore Industrial Networks Company

Contents.

1. Introduction
2. Voltcore - Context
3. Policy Objectives
4. Scope
5. Terminology
6. Types of Privileged Access
7. Core principles
8. Risks
9. Categories of Privileged Accounts
10. Tiered Administration Model
11. Legal and Regulatory Framework

Contents.

12. Technical Networks
13. Organizational Measures and Roles
14. Policies and Procedures
15. Privilege Granting Process
16. Control and Audit
17. SCADA-Specific Considerations
18. Incidents
19. Benefits
20. Limitations
21. Conclusion
22. References

2. Voltcore – context

VoltCore is an automated energy distribution organization.
Its core activities include:

- Management and monitoring of substations
- Control of energy flows
- Maintenance of SCADA systems
- Support and operation of infrastructure related to the operational environment

VoltCore operates within a hybrid infrastructure that combines a corporate IT network with an Operational Technology (OT) environment, where critical systems are managed.

3. Цели на политиката

- **Centralized management of privileged access** – The objective is to ensure that administrative access is not scattered across systems, but instead controlled through a unified and structured framework.
- **Minimization of abuse risk** – Employees should not have access to systems that require elevated privileges unless such access is strictly necessary for their work.
- **Enhanced protection of SCADA and critical infrastructure** – Access to key devices, configuration changes, and system-level modifications is minimized to the greatest extent possible.
- **Application of the "least privilege" principle** – Each individual is granted only the permissions required for their daily tasks, with no unnecessary access.
- **Action auditing** – All activities are logged to ensure traceability, including what actions were performed, when, by whom, and how, enabling retrospective review and verification.

4. Обхват

This policy applies to all individuals and technical accounts that, in any way, are granted elevated privileges within VoltCore systems.

IT administrators – Maintain servers and network infrastructure.

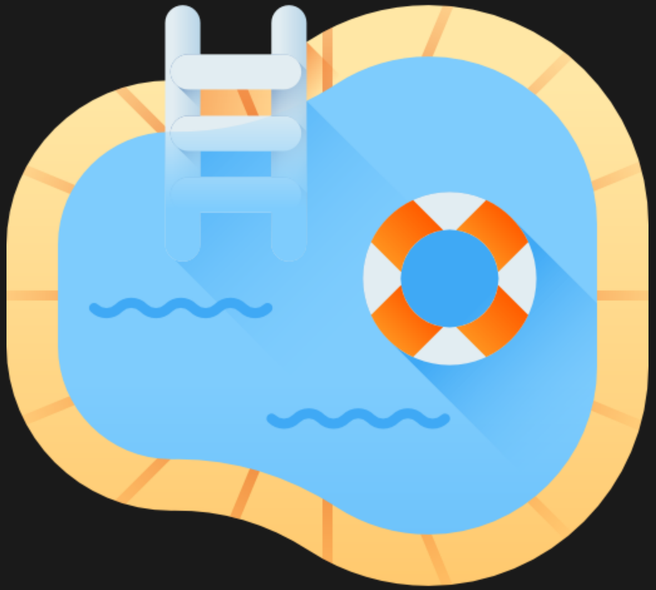
SCADA engineers – Work with equipment in the operational environment (PLC, RTU, HMI).

Operators – Use systems with elevated privileges for daily tasks, such as control panels and process monitoring.

External vendors – Provide maintenance or repair services; their access is also subject to this policy.

Service accounts (system accounts) – Used for various systems, automations, and integrations; require elevated privileges to function.

Remote access – Applies regardless of whether access is provided via VPN or through a dedicated Jump Host.



5. Терминология

Privileged access – Permissions used to modify settings, system files, or configurations. In short, access that allows you to “break or fix” something.

Lateral movement – A term describing movement within an environment, where an attacker transitions from one system to another by abusing privileges.

Jump host – A dedicated system through which administrative access is routed. The purpose is to prevent direct access to critical systems and instead enforce access through a controlled entry point.

Tier model – A hierarchical access structure. Tier 0 includes the most critical assets, followed by servers (Tier 1), and finally workstations (Tier 2).

Service account – An account created for a service rather than an individual user, typically used for automations or system integrations.

Break-glass account – A backup administrative account intended for emergency situations when standard access methods are unavailable.

SCADA – A system for monitoring and controlling industrial processes.
OT – Technologies that control and manage physical processes.
HMI – A system interface used for monitoring and controlling processes.
PLC – An industrial controller used to automate machines and processes.
RTU – A remote unit used for data collection and transmission to SCADA systems.
RDP – Microsoft’s Remote Desktop Protocol for remote computer access.
DMZ – Network segmentation that isolates the internal network from external networks.

6. Types of Privileged Access

System administration – Administrative access to operating systems, used for software installation, updates, configuration, and service management.

Configuration access (SCADA configuration) – Grants permissions to modify SCADA configurations, network settings, and other critical components.

Access to sensitive data – Provides the ability to manage information related to system configurations, personnel, and operational processes.

Access to OT devices (PLC/RTU) – Grants privileges to interact with the operational infrastructure, including controllers and equipment. Most users do not have any access to this environment.

Emergency access – Used only in emergency situations that require immediate action. Provides temporary elevated privileges when a system failure or critical issue demands urgent intervention.

7. Core Principles

- **Least privilege** – Only the permissions required to perform a specific task are granted.
- **Segregation of duties** – Critical changes must not be performed by a single individual.
- **Zero Trust** – There are no “trusted” zones; all access must be continuously verified.
- **Multi-Factor Authentication (MFA)** – A second authentication factor is required for administrative and SCADA access.
- **Tiered administration** – Administrative roles are separated based on their level of criticality.
- **Just-In-Time (JIT) access** – Privileges are granted only for a short, justified period of time.

8. Risks

- **Credential theft**
- **Pass-the-Hash / Pass-the-Ticket** – Use of captured hashes or authentication tickets
- Shadow admins
- Uncontrolled service accounts
- OT remote compromise
- RDP hijacking
- Lateral movement

9. Account Categories

Domain administrator – Accounts with the highest level of access across the entire domain environment. These are the most sensitive accounts and therefore require extremely strict security measures.

Local administrator – An administrator account with elevated privileges limited to a single machine, such as a workstation or a server.

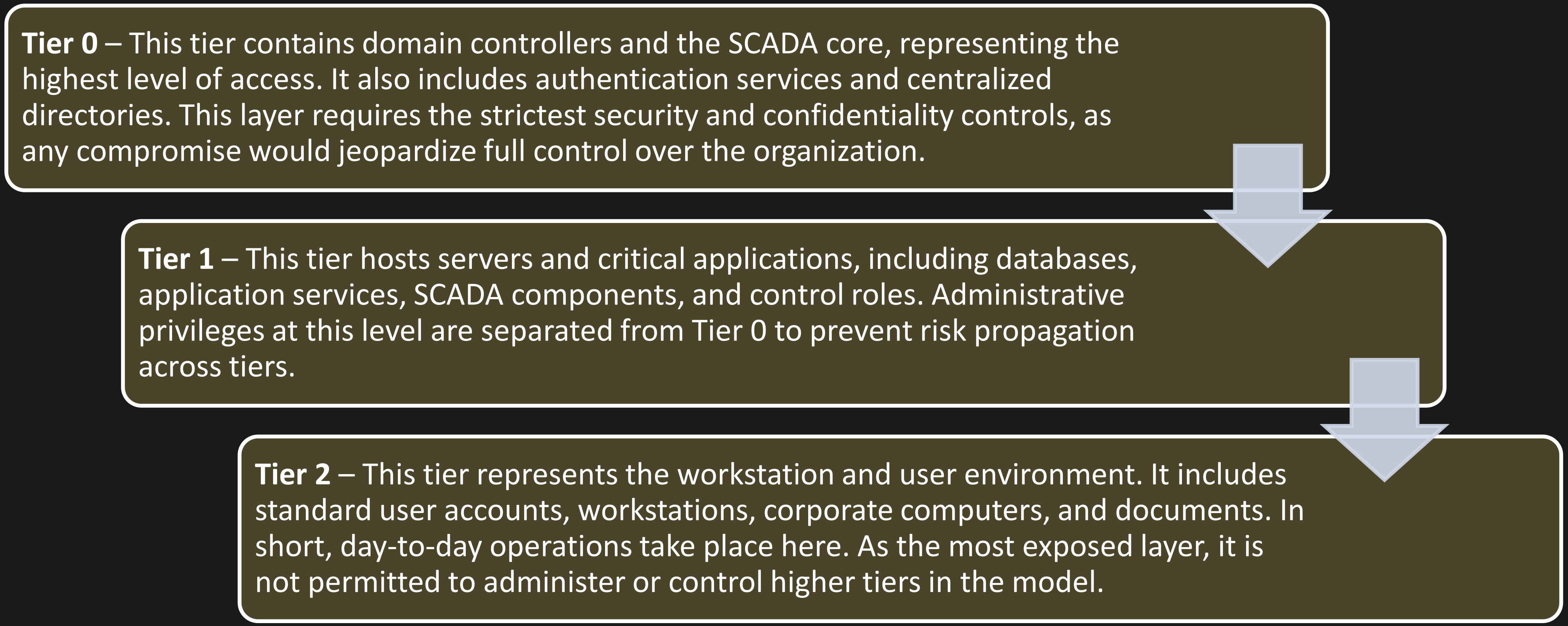
OT environment administrator (SCADA administrator) – Accounts responsible for managing SCADA servers, HMIs, PLC engineering workstations, and other OT systems.

Engineering accounts – Accounts primarily used by SCADA/PLC engineers to upload logic to PLCs, configure RTUs, perform testing, and monitor system configurations.

System accounts – Accounts intended for services, automations, and integrations. They are not created for use by individual employees.

Break-glass account (emergency administrative account) – These accounts remain locked and are used only in emergency situations. They may be activated if MFA fails or if standard administrative functions are unavailable. Their use follows a strict procedure and is always subject to mandatory post-incident auditing.

10. Tiered Model



Tier 0 – This tier contains domain controllers and the SCADA core, representing the highest level of access. It also includes authentication services and centralized directories. This layer requires the strictest security and confidentiality controls, as any compromise would jeopardize full control over the organization.

Tier 1 – This tier hosts servers and critical applications, including databases, application services, SCADA components, and control roles. Administrative privileges at this level are separated from Tier 0 to prevent risk propagation across tiers.

Tier 2 – This tier represents the workstation and user environment. It includes standard user accounts, workstations, corporate computers, and documents. In short, day-to-day operations take place here. As the most exposed layer, it is not permitted to administer or control higher tiers in the model.

11. Legal and Regulatory Framework

ISO/IEC 27001, Annex A.9 – This standard addresses access control and establishes the foundation for organizational access management rules.

NIST SP 800-82 (ICS Security) – A document focused on SCADA and industrial control systems, providing recommendations and guidance for designing and securing networks that manage critical components and controllers.

NIST SP 800-53 (Access Control – AC controls) – A standard for role-based access management, focusing on user privilege segmentation and mandatory system auditing.

CISA OT Network Segmentation Guidance – A set of recommendations on how to separate IT and OT environments, configure a DMZ, and restrict remote access to SCADA systems.

12. Technical Measures

Privileged Access Management (PAM) – Stores and manages administrative credentials and records privileged sessions.

Password rotation – A technique in which passwords are periodically changed to reduce the risk of credential compromise.

Session recording – Monitoring and recording of privileged sessions and the actions performed during them.

Jump server (intermediate server) – Users do not interact directly with target systems; all actions are performed through an intermediary server to ensure monitoring and traceability.

SIEM logging (audit system) – All performed actions are collected in a centralized system that monitors for unusual or risky activity and raises alerts when necessary.

Admin workstation (administrative workstation) – Dedicated machines designed for administrative tasks only; their use for daily work or non-administrative activities is prohibited.

Hardening – Systems are locked down for specific tasks, with all unnecessary processes disabled to minimize vulnerabilities as much as possible.

13. Organizational Measures and Roles

System administrators – Responsible for maintaining the entire infrastructure and implementing approved changes.

SOC (Security Operations Center) – Monitors and audits systems for suspicious activity and is responsible for responding to IT security incidents.

OT engineers – Responsible for maintaining SCADA systems and PLC/RTU environments, as well as the associated equipment and operational infrastructure.

Management – Ensures accountability at every stage, approves decisions before they are implemented, and governs access to system resources.

Service desk – Handles user access requests, registers them, and routes tickets to the appropriate teams.

- **Rules** – Define the boundaries for the use of system resources.
- **Procedures** – Describe the specific steps for requesting and granting access.
- **Roles and responsibilities** – Clearly define who performs which role and what responsibilities they hold in ensuring secure access.
- **Documentation** – Recording of access, reporting, and auditing during the granting of privileges.
- **Training** – Periodic staff training to improve risk awareness and reduce human error.

14. Policies and Procedures

Policies

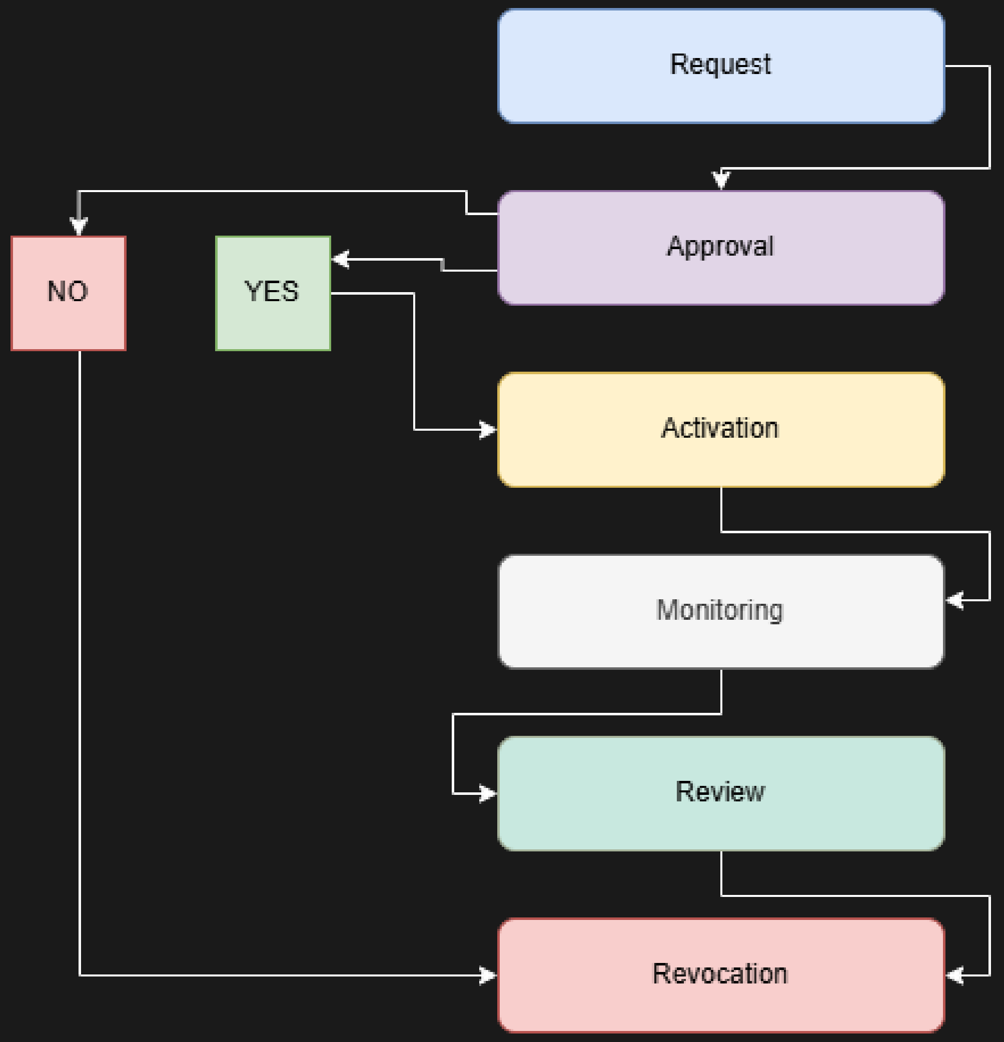
These are rules that govern the approval of different types of access. They define who is authorized to create changes and the requirements that must be followed to ensure secure access management.

Procedures

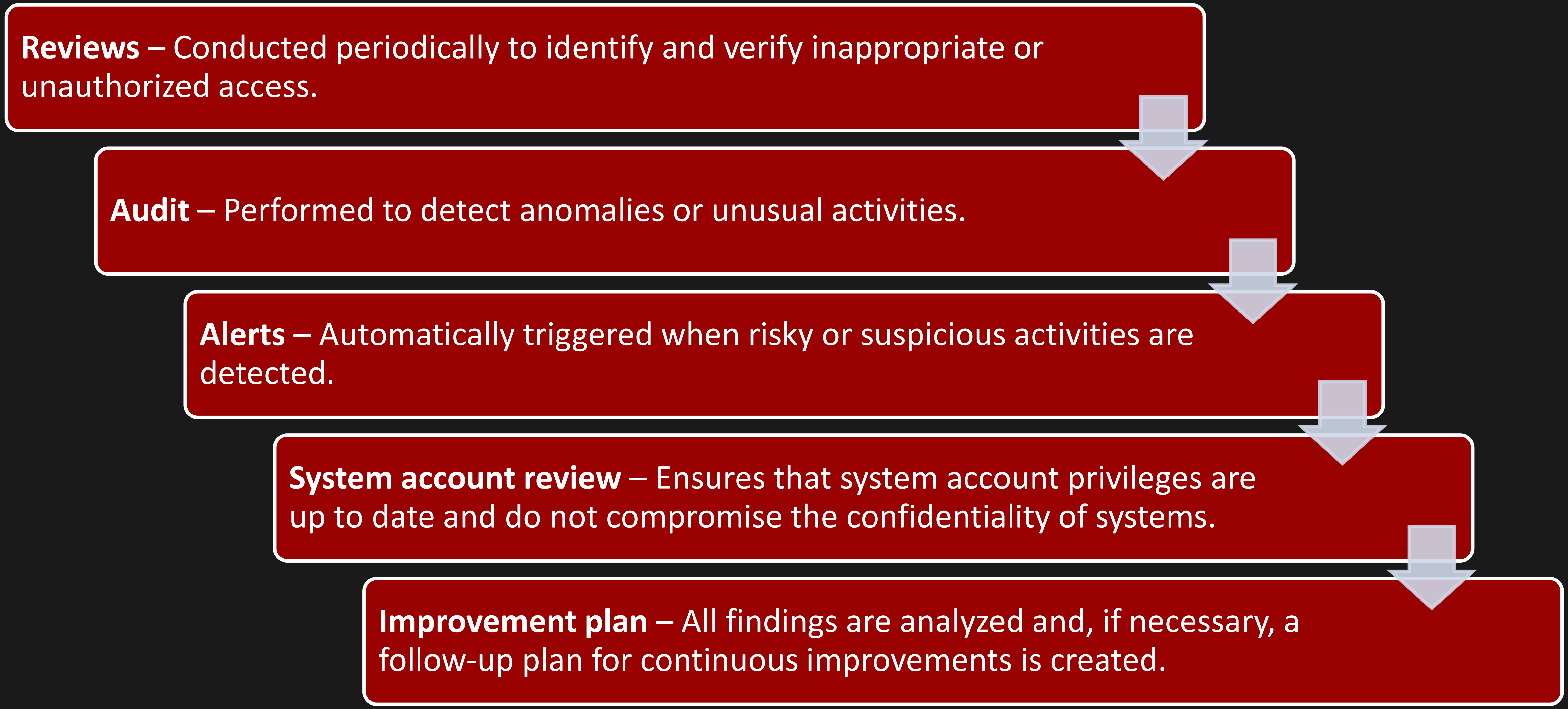
Defined steps followed when requesting access and during the review of access requests. They ensure controlled and traceable execution of actions, as well as proper documentation for audit and review. Access is revoked once it is no longer required, with records of when and why it was terminated, preventing unnecessary privilege accumulation.

15. Privilege Granting Process

1. An access request is submitted through the service desk, with a clear justification explaining why the privileges are required.
2. Management reviews the request to verify that the access is genuinely necessary.
3. If approved, an administrator grants temporary privileges and access is provided via a jump server, not directly to the target system.
4. Once access is granted, the system monitors and records all actions performed using the elevated privileges.
5. After a defined period, a review is conducted to confirm that the task has been completed and that the access is no longer required.
6. The access is then revoked to prevent unnecessary accumulation of privileges.



16. Control and Audit



Reviews – Conducted periodically to identify and verify inappropriate or unauthorized access.

Audit – Performed to detect anomalies or unusual activities.

Alerts – Automatically triggered when risky or suspicious activities are detected.

System account review – Ensures that system account privileges are up to date and do not compromise the confidentiality of systems.

Improvement plan – All findings are analyzed and, if necessary, a follow-up plan for continuous improvements is created.

17. SCADA-Specific Considerations

OT jump host – The operational environment is accessed only through a single, highly secured machine. This approach isolates sessions and significantly reduces risk.

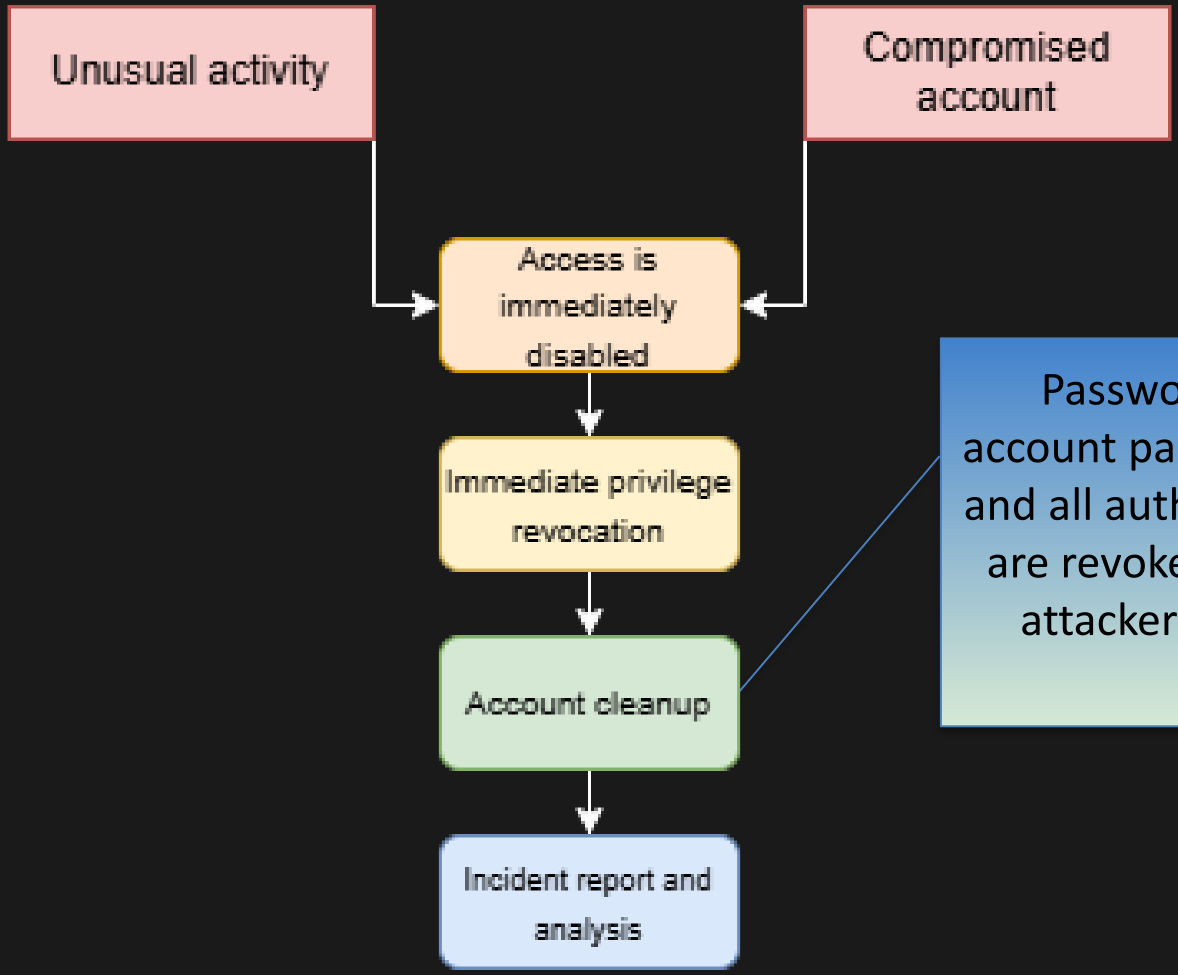
Read-only profiles – Operators use accounts with monitoring-only privileges, ensuring they cannot modify configurations.

DMZ segmentation – Even if a breach occurs somewhere in the system, the SCADA architecture is isolated within its own dedicated segment.

Physical access – Critical devices are stored in designated, access-controlled areas. A formal registration procedure is followed whenever physical access is granted.

Engineering sessions – Engineer access to restricted areas is performed under supervision, within a defined time window, and with a strictly controlled set of permitted commands and actions.

18. Incident Handling Procedure


Unusual activity
Compromised account
Access is immediately disabled
Immediate privilege revocation
Account cleanup
Incident report and analysis

Password reset – The account password is changed and all authentication tokens are revoked to prevent the attacker from regaining access.

19. Benefits

- Reduced risk
- Improved control
- Full traceability
- Strong protection ofSCADA infrastructure
- Fewer errors

20. Limitations

- High cost
- Training requirements
- Complex implementations
- Staff resistance (due to strict procedures and changes)

21. Conclusion

The Privileged Access Management policy is a vital element for preventing attacks, errors, and unauthorized access within the SCADA/OT critical infrastructures of the VoltCore organization. Through clear rules, structured workflows, continuous monitoring, and periodic reviews, the company can maintain a secure and resilient operational environment. Ultimately, the policy presented not only strengthens security but also contributes to more effective management of operations and organizational activities.

22. References

Guidelines and Standards

- ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Requirements
- ISO/IEC 27002:2022 — Code of Practice for Information Security Controls
- NIST Special Publication 800-82 Rev. 3 — Guide to Industrial Control Systems (ICS) Security
- NIST Special Publication 800-53 Rev. 5 — Security and Privacy Controls for Information Systems and Organizations
- CISA — Recommended Practices for OT Network Segmentation, 2022
- Microsoft — Privileged Access Strategy and Zero Trust Administration Models

Articles and Analysis

- MITRE ATT&CK for ICS — Official knowledge base: https://attack.mitre.org/matrices/ics/
- CISA ICS-CERT Advisories — https://www.cisa.gov/topics/industrial-control-systems

Professional Guides

CyberArk — Privileged Access Security: CyberArk Blueprint, 2023

BeyondTrust — Privileged Access Management for ICS/OT, Whitepaper

SANS Institute — ICS410: ICS/SCADA Security Essentials

Technical Documentation

Siemens — SCADA Architecture and OT Network Best Practices, Technical Guide

Schneider Electric — Industrial Control System Security Recommendations, 2021

Thank you for your time!

Prepared by: Martin Tsenkov