

Data Center “Biliki” and Hydro Power Plant “Mtkvari” Project

Information Security Architecture

(based on ISO/IEC 27001/27002:2022)

GE01-DES-PM08-GG-BOD-0002

Revision: 01

INDEX

INDEX	2
DEFINITIONS, ACRONYMS AND ABBREVIATIONS	3
1. Introduction	6
2. Objectives and Principles	6
3. Architectural Sections	7
3.1 Network Security	7
3.2 VPN Security	9
3.3 Virtualization Security	11
3.4 Data Storage Security	13
3.5 Access Management	15
3.6 Logging and Monitoring	16
3.7 Antivirus Strategy	18
3.8 Vulnerability Management	19
3.9 Vendor Security	20
3.10 Governance & Continuous Improvement	21
3.12 Asset Management	23
3.13 Encryption & Key Management	25
3.14 Incident Management	27
3.16 Security Awareness & Training	30
3.17 Physical & Environmental Security	31
3.18 Change & Configuration Management	33
3.19 Data Privacy & Protection	35
4. ISO/IEC Compliance	36
5. Conclusion	37

DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Acronym	Definition
ACL	Access Control List
ACS	Access Control System
AD	Active Directory
API	Application Programming Interface
BCP	Business Continuity Plan
CAB	Change Advisory Board
CAPA	Corrective and Preventive Actions
CIA	Confidentiality, Integrity, Availability
CMDB	Configuration Management Database
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DPA	Data Processing Agreement
DPI	Deep Packet Inspection
DPO	Data Protection Officer
DRP	Disaster Recovery Plan
EDR	Endpoint Detection and Response
GRC	Governance, Risk, and Compliance
HA	High Availability
HR	Human Resources
HSM	Hardware Security Module
IAM	Identity and Access Management
IDS	Intrusion Detection System

IEC	International Electrotechnical Commission
IPSec	Internet Protocol Security
IRT	Incident Response Team
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
KMS	Key Management System
LDAP	Lightweight Directory Access Protocol
MCLAG	Multi-Chassis Link Aggregation Group
MFA	Multi-Factor Authentication
MTTD	Mean Time To Detect
MTTR	Mean Time To Respond / Recover
NAC	Network Access Control
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OT	Operational Technology
OIDC	OpenID Connect
OS	Operating System
PAM	Privileged Access Management
PDCA	Plan–Do–Check–Act
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RCA	Root Cause Analysis
RADIUS	Remote Authentication Dial-In User Service
RPO	Recovery Point Objective

RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SD-WAN	Software-Defined Wide Area Network
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOAR	Security Orchestration, Automation and Response
SoD	Segregation of Duties
SOC	Security Operations Center
SSH	Secure Shell
TLS	Transport Layer Security
TPM	Trusted Platform Module
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WWN	World Wide Name
XDR	Extended Detection and Response

1. Introduction

This document defines the information security architecture of the organization ***** in accordance with international standards ISO/IEC 27001 and ISO/IEC 27002. The architecture aims to ensure the confidentiality, integrity, and availability of information resources, as well as to minimize risks and ensure regulatory compliance.

2. Objectives and Principles

Primary objectives of the security architecture:

- Establish a unified secure infrastructure.
- Provide multi-layered protection for data and services.
- Implement the principles of least privilege and segmentation.
- Enhance system resilience and manageability.

Core principles:

- Defense in depth
- Separation of duties
- Continuous monitoring and improvement
- Compliance with ISO/IEC 27001 / 27002 requirements

3. Architectural Sections

3.1 Network Security

Principles:

- Network architecture must follow multi-layered security and Zero Trust principles.
- Segmentation should minimize lateral threat movement and ensure isolation of critical resources.
- Redundancy and high availability ensure continuity of operations and minimize downtime.
- Configuration consistency must be maintained through standardized templates and automated provisioning.
- Network components and communication channels must use strong encryption and authenticated protocols only.
- Security controls must be centrally managed with full traceability and auditability.
- Any deviation from approved network design requires risk evaluation and formal change approval.

Requirements:

1. Define and document network zoning architecture (production, management, DMZ, OT, user, etc.).
2. Implement inter-zone traffic control using certified security tools.
3. Apply micro-segmentation to isolate workloads and services.
4. Ensure tenant isolation (multi-tenancy) at VLAN/VRF level.
5. Implement redundancy for network links and equipment.
6. Apply routing protocol authentication to prevent route table compromise.
7. Provide centralized management and monitoring of network infrastructure.

Implementation:

- A. Physical and logical HA of network infrastructure via HA clusters, MCLAG, and VRRP.
- B. Full traffic control (inbound, outbound, internal):
 - Border Firewall — control between external and internal zones.

- Internal Firewall — filter and analyze traffic between internal segments.
 - Virtual Firewalls (vFW) — control traffic in virtualized environments via Service Chaine.
 - Anti-DDoS systems to protect external perimeter.
- C. Tenant isolation via virtualized firewalls with dedicated Data Plane and Management Plane per customer
- D. Redundant communication paths using SD-WAN and IPSLA for automatic optimal route selection.
- E. Internal perimeter protection using DPI, Sandbox, Email Security, and advanced content filtering systems.
- F. All inter-zone and external communication over secure channels using TLS 1.3, IPsec, SSH.
- G. Centralized logging and correlation (SIEM) for continuous monitoring and incident detection.
- H. Regular audits and testing: configuration analysis, vulnerability scans, penetration testing.
- I. Network changes follow approved Change Management procedure with risk assessment and approval.
- J. Access control via device/user authentication (802.1X / NAC) with centralized access and rights management.
- K. Policies for log storage and analysis define retention periods, access, and incident response procedures.

3.2 VPN Security

Principles:

- Remote access must be secured equivalently to internal access.
- VPN sessions must be encrypted and authenticated.
- Administrative and user access must be segregated.
- Access is granted only after successful verification of identity, device compliance, and zntext (Zero Trust).
- VPN endpoints must be hardened, monitored, and verified for security state before session establishment.
- Split-tunneling must be restricted or prohibited unless formally justified and approved.
- VPN gateways must operate in high availability mode to ensure continuous secure access.
- VPN configuration and cryptographic parameters must follow organization-approved security standards and be regularly reviewed.

Requirements:

1. Use IPSec for Site-to-Site and Remote Access VPN.
2. Enforce Multi-Factor Authentication (MFA).
3. Dedicated VPN for administration.
4. Apply least privilege principle.
5. Maintain logs of all VPN sessions for auditing.

Implementation:

- A. Specialized agents on user OS ensure antivirus and security updates.
- B. Encrypted connection required for internal management system access (IPSec VPN).
- C. MFA mandatory.
- D. Full traffic control with routing to specific subnets via policies.
- E. VPN high availability via HA and redundant links.
- F. Site-to-Site VPN with certificate-based authentication if required.
- G. Remote portal for software updates if outdated.
- H. Full logging of connections with secure backup.

- I. Centralized key and certificate management via approved CAs, with rotation and validity control.
- J. VPN configurations and access policies periodically reviewed and tested.
- K. Continuous monitoring via SIEM/IDS with anomaly detection and alerts.

CONFIDENTIAL

3.3 Virtualization Security

Principles:

- Virtual environments must be secured with the same rigor as physical infrastructures.
- The hypervisor constitutes a high-value asset and must be protected with strict access, configuration control, and integrity monitoring.
- Workloads and tenants must be isolated at compute, storage, and network levels to prevent unauthorized access and lateral movement
- Only verified, trusted, and controlled virtual images and templates may be used in production.
- Security, performance, and resource allocation must be continuously monitored to detect anomalies and misuse.
- Administrative actions must be auditable and traceable, with role-based access enforcement and multi-factor authentication.
- Management networks and service networks must remain logically and physically isolated from tenant/user networks.
- Any changes to virtualization platforms must follow formal change management, review, and approval processes.

Requirements:

1. Deploy hardened hypervisors.
2. Restrict access to management consoles.
3. Ensure isolation at network and resource levels.
4. Apply integrity monitoring and updates.

Implementation:

- A. Hypervisors fully isolated; no direct storage on user disks.
- B. Hyperconverged architecture for easy VM migration and HA.
- C. Precise access control for users per configuration/resource.
- D. Traffic isolation via Service Chaining, virtual firewalls, and Private VLANs.
- E. Apply all security patches to hypervisors.
- F. Update policy enforcement.
- G. Host load limited to 60% to allow live migration for updates.
- H. Management, service, and user networks separated at hypervisor level.

- I. Network HA via Active-Backup.
- J. Monitoring, logging, SIEM integration mandatory.
- K. Access via least privilege with MFA for admins; all actions logged.
- L. Virtual images, templates, snapshots verified, scanned, and approved before production.
- M. VM/disk deletion follows secure data destruction procedures.

CONFIDENTIAL

3.4 Data Storage Security

Principles:

- Data protected throughout lifecycle.
- Access must be controlled and auditable.
- Data classification defines protection level and retention period.
- Integrity controls to prevent unauthorized modifications.
- Secure data disposal per approved policy with audit logging.

Requirements:

1. Encrypt data at rest and in transit.
2. Use RBAC for storage and access control.
3. Implement data classification policy with confidentiality levels and retention periods.
4. Ensure replication, backup, and recovery testing.
5. Define secure data deletion procedures.
6. Regularly test recovery and integrity.
7. Restrict storage access per roles and technical/administrative measures.
8. Log all data operations including admin actions and configuration changes.
9. Align storage with business continuity plans (BCP/DRP).

Implementation:

- A. HA networks and Multipath technology with iSCSI.
- B. Dedicated switches for SAN-server links with management/data traffic separation.
- C. SAN configured with WWN zoning and access restrictions.
- D. SafeMode/Retention periods; deletion only with at least two engineer confirmation.
- E. Backup critical data to separate storage or isolated segments.
- F. Backup testing with RTO/RPO and documented results.
- G. User accounts for each service with minimum rights (RBAC).
- H. Monitoring, logging, SIEM integration.
- I. Data integrity checks via checksums/hashes.
- J. All admin actions logged immutably.

- K. Classification levels (Public, Internal, Confidential, Critical) with retention and deletion rules.
- L. Secure deletion procedures with confirmation, logging, and certified tools.
- M. Storage and recovery policies aligned with BCP and regularly reviewed.

CONFIDENTIAL

3.5 Access Management

Principles:

- Access granted by identity and role, following least privilege principle.
- IT and OT domains separated.
- Privileged accounts under strict control.
- Formal processes for access provisioning, modification, and revocation.
- Critical system access granted only with approved necessity and time limit.

Requirements:

1. Centralized IAM with AD/LDAP, RADIUS, SAML, OIDC integration.
2. Temporary/approved privilege escalation (Just-In-Time Access).
3. Separate IT/OT authentication domains; no shared accounts.
4. Log all admin actions with user identity.
5. Periodically review/revoke inactive accounts/permissions.
6. MFA for all administrative/remote access.
7. Implement SoD (Segregation of Duties) to prevent conflicts.
8. Policy for password creation, change, lifespan, and storage.
9. Unique user IDs with assigned responsible persons.

Implementation:

- A. Formal password policy: complexity, length, rotation.
- B. PAM systems for privileged access control, action logging, task approval.
- C. High availability for PAM/IAM infrastructure.
- D. Network access to management subnets limited to PAM/admin IPs.
- E. Minimum user privileges per role/task.
- F. Logging and video recording of privileged actions, archived securely.
- G. Backup of logs and video archives in Cold storage with restricted access.
- H. Admin passwords stored securely with dual control.
- I. Automatic account lockout on suspicious activity, failed attempts, or inactivity.
- J. Regular access audits and remediation.
- K. Context-aware authentication (device, location, time, risk).
- L. PAM/IAM integrated with SIEM for anomaly detection.

3.6 Logging and Monitoring

Principles:

- Monitoring is key to incident detection and response.
- Logs provide evidential and analytical basis.
- Time synchronization critical for event correlation.
- Log control ensures completeness, immutability, timely processing.
- Monitoring systems must operate continuously and be protected from unauthorized access.

Requirements:

1. Centralized log collection in SIEM with event correlation.
2. Log retention: ≥ 1 year for security systems, ≥ 3 months for OS logs.
3. Synchronize infrastructure components via secure NTP.
4. Define severity levels, alerts, and escalation paths.
5. Automate incident response (SOAR).
6. Ensure log immutability and protection from deletion/modification.
7. Restrict access to logs and monitoring systems.
8. Log administrative actions and log access.
9. Regularly verify logging/monitoring completeness.
10. Integrate SIEM with IDS/IPS, EDR, DLP for comprehensive threat analysis.

Implementation:

- A. Centralized for log collection, analysis, correlation.
- B. HA SIEM infrastructure with database replication.
- C. Regular backup of all logs/metadata, including Cold Standby and isolated storage.
- D. Policy for backup, recovery, and retention.
- E. SOAR for automated response to critical events (IP block, host isolation, SOC notification).
- F. Internal NTP servers with limited external access.
- G. Log integrity via checksums, signatures, hashing.
- H. Separate audit logs for access control, firewalls, admin actions.
- I. SIEM integrated with IDS/IPS, EDR/XDR, SOC alerting.

- J. 24/7 monitoring with SLA-controlled response.
- K. Regular coverage assessment to ensure no critical system is outside monitoring.
- L. Log availability and timestamp accuracy tests during incident investigations.

CONFIDENTIAL

3.7 Antivirus Strategy

Principles:

- Multi-layered protection: signature, behavior, heuristic analysis.
- Threat detection and incident response integral to security.
- OT systems protected with minimal production impact.
- Antivirus events integrated with SIEM/SOAR.
- Centralized policy and update management ensures protection currency.

Requirements:

1. Deploy endpoint protection with signature, behavior, heuristic analysis.
2. Centralize antivirus policy and updates.
3. Apply application whitelisting for critical systems.
4. Integrate events into SIEM/SOAR.
5. Isolate and restore infected hosts, rollback to safe state.
6. Regular vulnerability assessment and policy compliance check.
7. Log antivirus actions/events for audit and investigation.
8. Protect against Zero-Day threats using EDR/XDR/Sandbox.

Implementation:

- A. Centralized antivirus management for timely updates.
- B. Regular controlled update of all devices.
- C. Monitoring and alerting integration.
- D. Internal system access only from devices with updated antivirus/security policies.
- E. Additional Zero-Day protection: EDR/XDR/Sandbox, proactive app behavior analysis.
- F. Periodic verification of antivirus databases/configurations.
- G. Incident response procedures: isolation, recovery, reporting.
- H. Verify protection across all endpoints including OT.
- I. Regular reports on security status and incidents for SOC and management.

3.8 Vulnerability Management

Principles:

- Infrastructure resilience achieved via timely vulnerability identification, analysis, and remediation.
- Remediation prioritization based on risk and asset criticality.
- Verification of vulnerability mitigation mandatory.
(ISO/IEC 27001: A.8.8; ISO/IEC 27002: 8.8, 5.30, 5.7)

Requirements:

1. Regular automated vulnerability scanning for all systems (network, servers, apps, virtual).
2. Prioritize remediation based on CVSS, risk context, and business impact.
3. Implement Patch Management Lifecycle: assessment → remediation → verification.
4. Maintain vulnerability registry with discovery date, responsible party, remediation status.
5. Define SLA per severity: critical ≤ 7 days, medium ≤ 30 days.
6. Document remediation verification and residual risks.
7. Quarterly reports on vulnerabilities and risks.
8. Periodic penetration testing and secure code analysis.
9. Exception process for temporary deviations with mandatory approval and registry entry.
10. Integrate results with SIEM/SOAR and GRC for automated reporting.

Implementation:

- A. Centralized scanning systems (Tenable, Qualys, Rapid7) with automated checks.
- B. Auto-feed critical vulnerability data to SIEM/GRC.
- C. SLA and overdue alerts configured.
- D. Quarterly penetration tests.
- E. Secure repository for remediation history/reports.
- F. Patch management and verification procedures.
- G. Trend analysis to identify recurring issues.

3.9 Vendor Security

Principles:

- External access/services must comply with internal security standards.
- Vendors responsible for security compliance and data confidentiality.
- Vendor monitoring and control continuous and documented.
- Vendors must report threats, incidents, or vulnerabilities impacting the organization.
- Interaction formalized via contracts, agreements, SLA.

Requirements:

1. Include security requirements in vendor contracts/agreements.
2. Authorize/control all external connections to the organization.
3. Define SLA for incident response, updates, remediation.
4. Regular audits of vendors for security compliance.
5. Immediate notification of incidents affecting organization.
6. Vendor staff must meet qualification requirements for critical systems.
7. Ensure spare equipment/services for rapid replacement.
8. Control vendor adherence to security policies on-site and remotely.

Implementation:

- A. Only trusted vendors with certifications.
- B. Vendor selection based on internal policies and risk assessment.
- C. 24/7 technical support from vendors.
- D. Rapid supply/spare component availability.
- E. Guaranteed SLA for response/remediation.
- F. Vendor personnel training and certification for equipment handling.
- G. Audit logging of all vendor actions.
- H. Periodic risk and compliance evaluation of vendors.
- I. Testing vendor interaction procedures, including incident simulations.

3.10 Governance & Continuous Improvement

Principles:

- Security evolves with infrastructure, technology, and threats.
- Governance aligns business goals with security requirements.
- Continuous improvement via PDCA (Plan–Do–Check–Act).
(ISO/IEC 27001:2022 — clause 10; ISO/IEC 27002:2022 — 5.35, 5.36; NIST CSF — GV)

Requirements:

1. Create Cybersecurity Design Review Board (CDRB) for key decisions and architecture approval.
2. Conduct annual and ad-hoc risk assessments, updating asset/threat registers.
3. Follow NIST CSF, ISO/IEC 27001, IEC 62443, integrating into corporate governance.
4. Consider incidents, audit results, and testing outcomes in planning new projects.
5. Define and review KPI/security metrics for ISMS effectiveness.
6. Maintain improvement register and corrective action plans based on incidents/audits.
7. Quarterly security effectiveness reviews by management.
8. Change Management with security impact assessment.
9. Internal audits and ISO/IEC 27001 self-assessment.
10. Document all CDRB decisions and track implementation.
11. Develop/update IS security roadmap per strategic goals and threat trends.

Implementation:

- A. CDRB committee with regular meetings and minutes.
- B. PDCA cycle: analysis, corrective actions, follow-up control.
- C. GRC platform for change, risk, and improvement management automation.
- D. Annual IS maturity report and recommendations.
- E. Lessons Learned methodology applied post-incidents/audits.
- F. Include improvements in budgeting and strategic IS planning.

3.11 Risk Management

Principles:

- Security decisions based on risk assessment results.
- Balance protection, cost, and operational efficiency.
- Risk-based approach throughout IS lifecycle.
- Minimize residual risk to acceptable levels.
- Risk register and assessments documented and updated regularly.

Requirements:

1. Implement ISO/IEC 27005-based risk assessment methodology.
2. Classify risks by likelihood and impact.
3. Define acceptable residual risk (risk appetite).
4. Assign risk owners and asset custodians.
5. Conduct planned/ad-hoc risk reviews after infrastructure/policy changes or incidents.
6. Implement mitigation measures with priorities and timelines.
7. Integrate risk management into corporate GRC.
8. Inform management of key risks and trends.
9. Store risk assessment and review results in centralized secure storage.

Implementation:

- A. Centralized risk register: threats, assets, vulnerabilities, likelihood, impact.
- B. Annual or event-driven register review.
- C. GRC automation for risk analysis/monitoring.
- D. Management reports on risk trends and mitigation effectiveness.
- E. Evaluate effectiveness of controls and update risk plans.
- F. Response scenarios and high-risk mitigation plans.
- G. Quantitative and qualitative risk analysis (e.g., probability/impact matrix).
- H. Traceability between risks, assets, and security controls.
- I. Staff training on risk identification and management in their area.

3.12 Asset Management

Principles

- Asset management should cover the full lifecycle, from acquisition and deployment to maintenance, transfer, and decommissioning.
- Asset owners are responsible for the accounting, protection, and correct operational use of assigned assets.
- The organization must maintain accurate, up-to-date records of all assets, including virtual, cloud, and outsourced components.
- Asset handling must comply with applicable regulatory, contractual, and internal security requirements.
- Only authorized personnel may access or modify asset records, with corresponding audit trails and approval workflows.
- Asset data must be validated regularly to ensure consistency, detect discrepancies, and prevent untracked (shadow IT) resources.
- Changes in asset status (ownership, location, configuration, disposal) must follow documented procedures and be traceable in the CMDB.

Requirements

1. Maintain a centralized asset registry (CMDB) including hardware, software, data, licenses, accounts, and cryptographic keys.
2. Assign asset owners, determine criticality, and classify according to CIA (Confidentiality, Integrity, Availability).
3. Include both physical and logical assets, including cloud and virtual resources.
4. Define acceptable use policies for assets, including rules for storage, access, and data transfer.
5. Establish procedures for asset transfer and return during role changes, employee termination, or third-party handover.
6. Implement procedures to ensure the asset registry is up-to-date and perform annual audits at a minimum.
7. Implement secure asset disposal processes ensuring data deletion or destruction.

Implementation

- A. Integrate CMDB with monitoring, SIEM, and ITSM systems for automated asset data updates.
- B. Automate new asset registration and regular verification of the registry at IT and security levels.
- C. For critical assets — enforce backup, encryption, and access control based on least privilege.
- D. Implement procedures for secure decommissioning of equipment and documentation of disposal.
- E. Conduct annual audits of asset status and discrepancy analysis.

CONFIDENTIAL

3.13 Encryption & Key Management

Principles

- Confidential data must be protected with strong encryption throughout its lifecycle: storage, transmission, processing, and disposal.
- Choice of algorithms and key lengths must comply with legal requirements, corporate policies, and international security standards.
- Key management must ensure integrity, availability, and confidentiality of cryptographic materials.
- Processes for key generation, storage, usage, rotation, and destruction must be formalized and documented.

Requirements

1. Use certified cryptographic tools.
2. Store keys only in secure cryptographic modules (HSM, KMS, TPM).
3. Define roles and responsibilities for key management (Key Custodian, Security Officer).
4. Establish regulations for key generation, distribution, rotation, backup, and destruction.
5. Apply segregation of duties for master key operations (dual control).
6. Record and audit all key-related operations.
7. Regularly verify compliance of algorithms and parameters with corporate crypto-policy.
8. Store encrypted key backups in secure physical or hardware repositories.
9. Encrypt all backups, administrative traffic, and user data.

Implementation

- A. Deploy centralized KMS/HSM systems with role-based access and mandatory administrator audit.
- B. Mandatory encryption of all backups, administrative traffic, and configuration data.

- C. Conduct regular audits of cryptographic infrastructure compliance with corporate policy and standards.
- D. Automate key rotation and revocation via KMS integration with PKI systems.
- E. Use segregated storage for master keys with restricted physical and logical access.
- F. Develop a cryptographic information protection policy, including approved algorithms, key lengths, expiration, and destruction procedures.
- G. Implement mechanisms to prevent key compromise (e.g., key splitting, dual-admin access).
- G. Regularly test key recovery and rotation procedures as part of business continuity planning (BCP).

CONFIDENTIAL

3.14 Incident Management

Principles

- Every information security incident must be promptly detected, recorded, classified, investigated, and resolved.
- Incident management should ensure continuous improvement of protection and reduction of response time.
- Investigation results should be used to prevent recurrence and improve security measures.
- Responsibilities and procedures must be clearly defined and documented.
- Communication about incidents must be timely and follow an escalation matrix.
- Lessons learned should feed into risk assessments and security awareness programs.

Requirements

1. Implement a unified incident management process per ISO/IEC 27035.
2. Ensure classification, categorization, and prioritization of incidents based on criticality and impact.
3. Define SLA levels for response and recovery.
4. Assign responsible persons and response teams (IRT/CSIRT).
5. Register all incidents in a centralized system and maintain investigation history.
6. Perform root cause analysis (RCA) and document results.
7. Develop and maintain standard response playbooks for typical threats.
8. Integrate incident management with SIEM/SOAR, event correlation, and ticketing systems.
9. Establish notification procedures for management and external parties, including clients, regulators, and partners, for significant incidents.
10. Conduct regular exercises and testing of response procedures.
11. Train personnel to identify and report suspicious events promptly.
12. Use metrics (MTTD, MTTR, SLA performance) to evaluate response effectiveness.

Implementation

- A. Use a ticketing system integrated with SIEM and SOAR for registration, classification, and automated response.

- B. Assign responsible persons and response teams with clear accountability.
- C. Conduct post-incident reviews, documenting findings and corrective actions.
- D. Develop and maintain playbooks for common incidents (account compromise, malware, DDoS, data leakage).
- E. Store complete incident history and reports in a secure centralized repository.
- F. Integrate with alerting and escalation systems to inform responsible parties.
- G. Regular training and simulation for all participants.
- H. Monitor implementation of corrective actions and update security policies based on lessons learned.

CONFIDENTIAL

3.15 Compliance & Audit

Principles

- Compliance with international and internal standards is mandatory for the information security system.
- Audits must be conducted regularly, objectively, and with participation of independent parties.
- Audit results are used for continuous improvement of security systems.

Requirements

1. Conduct regular internal and external audits per approved plan (at least annually).
2. Appoint independent auditors or engage accredited external organizations.
3. Maintain a record of nonconformities and corrective actions, tracking their resolution.
4. Ensure compliance with ISO/IEC 27001, ISO/IEC 27002, and local legal requirements (e.g., personal data).
5. Assess effectiveness of security measures after audits.
6. Retain evidence of compliance (protocols, reports, acts).
7. Document audit process and approve reports by management.
8. Periodically review policies and procedures based on audit results.

Implementation

- A. Implement a GRC platform to automate audits, risk management, and compliance processes.
- B. Generate annual compliance reports highlighting nonconformity trends and remediation progress.
- C. Conduct employee training based on audit results and identified nonconformities.
- D. Implement corrective and preventive actions (CAPA).
- E. Configure alerts for certification review and renewal deadlines.
- F. Restrict access to audit documents and confidential information to authorized personnel only.

3.16 Security Awareness & Training

Principles

- People are a key element of security.
- Awareness reduces the likelihood of incidents and internal breaches.
- Training should be continuous, relevant, and role-based.

Requirements

1. Conduct quarterly security awareness training for all employees.
2. Test employees' knowledge and document results.
3. Conduct regular phishing tests and social engineering drills.
4. Track course and certification completion.
5. Train contractors, temporary staff, and service personnel before granting access.
6. Update training programs with emerging threats, technologies, or incidents.
7. Include real incident cases and violation examples in training.
8. Evaluate the effectiveness of awareness programs.

Implementation

- A. Develop an e-learning platform with role-based scenarios and automated results tracking.
- B. Regularly assess employee knowledge and analyze weaknesses.
- C. Conduct incident response and cyber hygiene training.
- D. Integrate training program with HR systems to track employee status.
- E. Run simulated phishing campaigns with post-analysis.
- F. Update training content based on threat and incident changes.
- G. Generate management reports on progress and employee engagement.

3.17 Physical & Environmental Security

Principles

- Physical protection of data centers and workspaces is fundamental to cybersecurity.
- Protection must address unauthorized access as well as natural, technological, and internal threats.
- Access to sensitive areas must be controlled, logged, and periodically reviewed.
- Environmental hazards (fire, water, temperature, humidity, power) must be monitored and mitigated.
- Security measures should support business continuity and disaster recovery plans.
- Responsibilities for physical security must be clearly assigned and enforced.

Requirements

1. Control access using ACS and CCTV.
2. Ensure fire protection and climate control.
3. Develop evacuation and emergency response plans.
4. Record and store physical access logs with audit capability.
5. Restrict personal devices and removable media in secured areas.
6. Regulate escorting of third-party personnel and contractors in secure zones.
7. Protect cabling infrastructure and racks from unauthorized access.

Implementation

- A. Deploy multi-level access control systems.
- B. Mandatory user authentication via entry gateway to data centers.
- C. Define procedure for requesting and approving physical access.
- D. Implement redundant power and cooling systems.
- E. Regularly test emergency procedures.
- F. Record all personnel entries/exits with logs stored at least 6 months.
- G. Establish equipment intake zones with device and media movement control.
- H. Periodically inspect CCTV and back up recordings.

- I. Implement response procedures for physical incidents (break-ins, fire, leakage, etc.).

CONFIDENTIAL

3.18 Change & Configuration Management

Principles

- All changes must be controlled, tested, and documented.
- Configurations must be maintained in an up-to-date, secure, and auditable state.
- System security should be evaluated before, during, and after changes.
- Changes must follow the principle of least disruption to services and business operations.
- Responsibilities for change approval, implementation, and verification must be clearly assigned.
- Unauthorized or ad-hoc changes are strictly prohibited.
- Audit trails of changes must be retained for compliance and incident investigation purposes.

Requirements

1. Establish a centralized change approval process (CAB — Change Advisory Board).
2. Maintain version control and rollback capability.
3. Perform impact analysis (including security risk assessment) before changes.
4. Assign responsibilities for implementation, verification, and documentation.
5. Separate rights for initiating, approving, and executing changes (4-eyes principle).
6. Test changes in an isolated staging environment.
7. Inventory all configurations with versions, owners, and statuses.
8. Automate configuration compliance checks against security policies.
9. Periodically audit and analyze change management effectiveness.

Implementation

- A. Use ITSM platforms (e.g., ServiceNow) for change registration and approval.
- B. Maintain change logs with author, date, and description.
- C. Configure automatic backup of configurations before each change.
- D. Conduct impact analysis and test changes in a controlled environment before deployment.
- E. Separate roles among developers, administrators, and auditors.

- F. Centralize storage and version control of configuration files.
- G. Periodically compare current configurations with baseline and automatically alert deviations.
- H. Support rollback procedures if errors are detected.

CONFIDENTIAL

3.19 Data Privacy & Protection

Principles

- Personal and confidential data must be processed with principles of minimization, legality, and transparency.
- Access is granted strictly on a need-to-know basis (principle of least privilege).
- Data processing must be documented and controlled at all stages.

Requirements

1. Comply with ISO/IEC 27701 and local data protection laws (e.g., GDPR).
2. Control data transfer to third parties, including DPA/NDA agreements.
3. Ensure data subject rights: access, correction, deletion, portability.
4. Appoint a Data Protection Officer (DPO) and define responsibilities.
5. Define retention periods and secure deletion of personal data.
6. Implement encryption and pseudonymization for storage and transmission.
7. Establish timely data breach notification procedures.
8. Train employees on privacy and personal data handling.

Implementation

- A. Deploy DLP systems and data protection policies.
- B. Conduct periodic audits of personal data processing and storage.
- C. Perform DPIA (Data Protection Impact Assessments).
- D. Appoint a DPO and document roles/responsibilities.
- E. Encrypt personal data in storage, backups, and transmission.
- F. Develop secure deletion and anonymization procedures.
- G. Implement automated notifications for personal data incidents.
- H. Conduct regular staff training on personal data handling and ISO/IEC 27701 compliance.

4. ISO/IEC Compliance

No	Section	ISO Standard Compliance
3.1	Network Architecture & Segmentation	ISO/IEC 27001: A.13.1, A.13.2; ISO/IEC 27033
3.2	VPN Security	ISO/IEC 27033-3; ISO/IEC 27002: A.13.1.1, A.13.2.3
3.3	Access Control	ISO/IEC 27001: A.9; ISO/IEC 27002: 9.1–9.4
3.4	Authentication & Account Management	ISO/IEC 27002: 9.2.1–9.2.6, 9.4.2
3.5	Logging & Monitoring	ISO/IEC 27001: A.12.4; ISO/IEC 27002: 12.4.1–12.4.3
3.6	Backup Management	ISO/IEC 27002: 12.3; ISO/IEC 27040
3.7	Malware Protection	ISO/IEC 27002: 12.2; ISO/IEC 27035
3.8	Vulnerability Management	ISO/IEC 27002: 12.6; ISO/IEC 27005
3.9	Change & Configuration Management	ISO/IEC 27002: 12.1.2, 12.5.1
3.10	Management & Improvement	ISO/IEC 27001: 9.1–10.2
3.11	Risk Management	ISO/IEC 27005; ISO/IEC 27001: 6.1.2
3.12	Encryption & Key Management	ISO/IEC 27001: A.10; ISO/IEC 19790; FIPS 140-2
3.13	Incident Management	ISO/IEC 27035; ISO/IEC 27001: A.16
3.14	Compliance & Audit	ISO/IEC 27001: 9.2–10.1; ISO/IEC 27014
3.15	Security Awareness & Training	ISO/IEC 27001: 7.2; ISO/IEC 27002: 7.2.2
3.16	Physical & Environmental Security	ISO/IEC 27001: A.11; ISO/IEC 27002: 11.1–11.2
3.17	Supplier & Contractor Management	ISO/IEC 27036; ISO/IEC 27002: 15.1–15.2
3.18	Change & Configuration Management	ISO/IEC 27001: A.12.1.2; ISO/IEC 20000
3.19	Data Privacy & Protection	ISO/IEC 27701; ISO/IEC 27018; GDPR (if applicable)

5. Conclusion

This architecture forms the foundation for a secure, resilient, and ISO-compliant infrastructure for **Data Center “Biliki” and Hydro Power Plant “Mtkvari” Project**.

Its implementation ensures a high level of protection, manageability, and cyber resilience.

This document, prepared for the deployment of information security policies and procedures, guarantees that implemented measures comply with international standards ISO/IEC 27001, ISO/IEC 27002

The Information Security Management System demonstrates:

- High maturity in risk, asset, and incident management;
- Compliance with core principles of confidentiality, integrity, and availability;
- Existence of continuous improvement and audit procedures.