Everest Group®

Technical and Organizational Measures

Everest Group exercises several technical and organizational measures. These include the following:

Access Control	A user access management lifecycle process cover: a) joiners, movers, leavers b) privileged and non-privileged access c) periodical review / recertification d) approval routines e) process monitoring f) make sure that only individual and unique accounts are allowed
Access Control Mechanisms	Access to information systems requires strong / two factor authentication. The product/service support standardized access control integration mechanisms, such as Kerberos and SAML.
Application Protection	Product/service are protected against unauthorized access to information by: a) hardening by ensuring that all unnecessary software, network services and applications have been disabled/removed b) providing 'defence in depth' (i.e., using multiple layers of different types of protection) to avoid reliance on one type or method of security control c) only allowing access to Supplier services from customers corporate network (as opposed to from e.g., employees home PC(s).
Asset Register	All hardware / software recorded in an accurate and up-to-date asset register
Backup	There is a standards/procedure for performing backups, which cover: a) the types of information and software to be backed up b) backup cycles d) protection of backups
Browser-based Application Protection	The product/service shall be developed as per standard guidelines and continuously protected against risks/vulnerabilities.
Change Management	A change management process is established, which covers all types of change (e.g., upgrades and modifications to application and software, modifications to business information, emergency 'fixes', and changes to information systems and networks) covering: - approval by authorized manager - impact analysis - testing - back-out plan Product updates must be tested, reviewed and applied using a change management process.
Consumer Devices and BYOD	Standards/procedures are in place to ensure critical and sensitive business information handled on consumer devices receives the same level of protection as that typically provided for mobile devices (e.g., laptops).
Crisis Management	The crisis management process: a) include steps to be taken in a crisis or emergency situations b) provide contact details for all key individuals (including those in the crisis management team and those associated with external parties such as law enforcement agencies, industry regulators and organizations in the supply chain) c) be rehearsed and tested on a regular basis, using real life simulations.
Cryptographic Key Management	There is a documented standards/procedures for managing cryptographic keys, which cover: a) the lifecycle of cryptographic keys b) responsibilities of cryptographic key owners c) protection of cryptographic keys Cryptographic keys are securely managed and protected against unauthorized access or destruction

Cryptographic Solutions	Cryptography is used for data in transit and at rest across the organization to: - protect the confidentiality of sensitive information or information that is subject to legal and regulatory-related encryption requirements (e.g. Payment Card Industry Data Security Standard (PCI DSS) and European Commission Directive 95/46/EC) -Cryptographic solutions are subject to approval
Customer Access Arrangements	There are standards/procedures for the provision of access to the organization's business applications by customers
Cybercrime Attacks	There are procedures for dealing with cybercrime attacks.
Email	Email and instant messaging systems are protected to ensure that they are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimized.
Emergency Fixes	There are standards/procedures for applying emergency fixes to business information, business applications and technical infrastructure (including systems software and computer equipment). Emergency fixes must be approved by an appropriate business representative, logged, and carried out in accordance with standards/procedures
External Network Connections	All external network connections to information systems and networks are individually identified, verified, recorded, and approved by the information systems or network owner.
External Supplier Management Process	There is a documented process for managing the information risks associated with external suppliers (including hardware, software, outsourcing and cloud services).
Firewalls	Firewalls protect networks by having network traffic routed through the firewall prior to accessing networks, or before leaving networks.
Hazard Protection	Critical facilities (including locations that house computer systems such as data centres, networks, telecommunication equipment, sensitive physical material and other important assets) are protected against fire, flood, environmental and other natural hazards.
Information Classification	An information classification scheme is being established that applies throughout the organization, based on the confidentiality, integrity and availability of information.
Information Leakage Protection	Information leakage protection mechanisms has been employed for information systems and networks that process, store and transmit sensitive information.
Information Security Assurance Programme	Information security activities have been established, which assures that: a) security requirements are identified based on information classification, information risk assessment and compliance requirements (legal/regulatory/contractual) b) identified risks are treated in accordance with business requirements, and any accepted risks subjected to sign-off by the business c) relevant security controls are implemented d) information risk is managed as part of the organization's project management methodology e) the effectiveness and efficiency of security arrangements is monitored and reported to the governing body
Information Security Incident Management	Information security incidents are identified, responded to, recovered from, and followed up (including forensic investigations) using an information security incident management process.

Information Security Policy	We have an Information security policy that applies across the organization, and defines information security, associated responsibilities and the information security principles to be followed by all staff. A dedicated team manages the Information security and reports to the CTO, who reports directly to the CEO)
Intrusion Detection	Intrusion detection mechanisms have been applied to high-risk information systems and networks.
Legal and Regulatory Compliance	A process has been established for ensuring the product/service compliance, which covers: a) discover laws and regulations that affect information security b) interpret the information security implications of discovered laws and regulations c) identify potential legal/regulatory non-compliance (e.g. performing a risk assessment of compliance with laws and regulations) d) address areas of potential legal/regulatory non-compliance.
Local Security Co-ordination	Responsibility for information security is assigned to the individual in charge of each local business unit or department
Malware Protection Software	Effective malware protection software has been installed, configured, and maintained throughout the organization.
Managing Information Risk Assessment	Standards/procedures are laid out for performing information risk assessments, which apply across the organization.
Mobile Device Configuration	Mobile devices (including laptops and consumer devices) are managed by standards/procedures, which cover: a) system configuration (e.g. securing the firmware and employing standard builds) b) provision of software to protect them (e.g. system management tools, access control mechanisms, malware protection software and encryption capabilities) c) protection of the memory of computing devices against misuse and attack d) use of encryption to protect sensitive information e) configuration of event logging.
Monitoring Information Security Compliance	Standards/procedures covers: a) identifying the security compliance obligations b) translating obligations into compliance-related information security requirements and controls c) implementing security controls to meet obligations d) monitoring compliance-related information security controls e) reporting results of monitoring activities and recommending actions to mitigate compliance risks.
Network Device Configuration	Procedures are in place for configuring network devices (e.g., routers, hubs, bridges, concentrators, switches and firewalls), which cover: a) device configuration b) restricting access to network devices c) vulnerability and patch management d) regular review of network device configuration and set-up.
Office Equipment	Office equipment are managed by standards/procedures, which covers: a) deployment and physical protection of office equipment b) restricting access to sensitive equipment c) monitoring the use of office equipment d) encrypting information transmitted to and processed by office equipment e) decommissioning office equipment in a secure manner.
Physical Network Management	Network cables and network access points have been protected to prevent unauthorized users from gaining access to information systems and networks

Physical Protection	Standards/procedures covers: a) protecting critical facilities against unauthorized access b) locating critical facilities away from public access or approach c) restricting access to critical facilities that support or enable the organization's critical infrastructure d) managing authorization for physical access to critical facilities e) restricting visitor access to critical facilities. Buildings that house critical facilities are protected against unauthorized access by: a) providing locks, bolts (or equivalent) on vulnerable doors and windows and employing security guards b) installing closed-circuit television (CCTV), or equivalent c) locating intruder detection systems on accessible external doors and windows and testing regularly.
Portable Storage Devices	The use of portable storage devices (e.g., USB memory sticks, external hard disk drives, media players and e-book readers) are subject to approval, access to them restricted, and information stored on them protected.
Power Supplies	Critical facilities (including locations that house computer systems such as data centers, networks, telecommunication equipment, sensitive physical material and other important assets) are protected against power outages.
Quality Assurance	Quality assurance of the product/service development methodology include: a) checking that security requirements b)) confirming that security controls have been developed and are working correctly c) confirming that individuals responsible for developing, testing and implementing systems under development are following the system development methodology
Remote Environments	Staff working in remote environments (e.g., in locations other than the organization's premises) must be subject to authorization, protect computing devices against loss and theft, be supported by security awareness material, and employ additional controls when travelling to high-risk countries or regions.
Remote Maintenance	Remote maintenance of systems and networks are restricted to authorized and strongly authenticated individuals, confined to limited time period, subject to logging of all activity undertaken, and periodically reviewed.
Roles and Responsibilities	Ownership of critical and sensitive information, business applications, information systems and networks must be assigned to individuals (e.g., business managers), and the responsibilities of owners documented. Responsibilities for protecting critical and sensitive information, business applications, information systems and networks must be communicated to and accepted by owners.
Security Audit Management	Independent security audits must be performed regularly for target environments that are critical to the delivery to customer.
Security Audit Process – Planning	Customer internal or external auditors have right to initiate an examination of administrative (regulations, plans, policies) as well as technical adoption of the security regulations on site at the Supplier.
Security Awareness Messages	Individuals who have access to the information and systems of the organization have tailored and appropriate security messages communicated to them on a regular basis.
Security Awareness Programme	A security awareness trainings are periodically conducted to promote security awareness throughout the organization and establish a positive security culture.
Security Event Logging	Security related events (including event types such as failed login attempts, system crash, deletion of user account and event attributes such as date, time, UserID, file name, IP address) are recorded in logs by the product/service and protected against unauthorized change.

Security Testing	Product/services are subject to testing the security of systems under development, which include: a) performing independent security checks of the application code b) sign-off of the results of code review c) determining the effectiveness of security controls d) performing specific attack tests to identify weaknesses in browser-based applications e) using test data for security testing f) resolving of flaws and security weaknesses identified during code review and testing. g) sign-off of flaws and security weakness mitigations.
Server Configuration	Servers have been configured in accordance with standards/procedures, which covers: a) providing standard firmware configurations b) using standardized, predetermined server images to build/configure servers c) changing Supplier defaults and other security parameters d) disabling or restricting unnecessary functions and services e) restricting access to powerful system utilities and host parameter settings f) protecting against unauthorized access
Specifications of Requirements	The development methodology of the product/service includes specification of requirements to protect the confidentiality, integrity and availability of information throughout its lifecycle in the product/service, including: a) creation (e.g. input validation) b) processing (e.g. integrity checking and performance) c) storage (e.g. location and access control) d) transmission (e.g. source and destination checking) e) destruction (e.g. secure erasure).
Staff Agreements	Terms and conditions of employment must: a) state that information security responsibilities extend outside normal working hours and premises, and continue after employment has ended b) explain the employee's legal responsibilities and rights (e.g. regarding copyright laws, data protection or privacy legislation) c) require the employee to adhere to the organization's information security policy and supporting policies (e.g. acceptable usage policies) d) include a non-disclosure/confidentiality clause. Applicants for employment (including internal staff and external individuals such as consultants, contractors, engineers and employees of external parties) are screened prior to commencing work (e.g. by taking up references, checking career history/qualifications and confirming identity, such as by inspecting a passport.
System and Software Vulnerability Management	Standards/procedures have been established for system and software vulnerability management
System Development Environments	Application source code (or equivalent) used in development environments are protected by: a) preventing development staff from making unauthorized changes to live environments (e.g., by using access control software) b) applying strict version control over systems development software (e.g,. by using configuration management, recording access in a log and archiving old versions of software regularly) The system development methodology (often referred to as the systems development lifecycle (SDLC)), is based upon sound systems development and project management practices.

User Authorization	The processes for authorizing users: -have been defined in writing, approved by the relevant owner and applied to all users - have associate access privileges with defined users (e.g. using unique identifiers such as UserIDs) - have assigned users with default access based on the principle of least privilege (e.g. 'none' rather than 'read') -ensure redundant identifiers (e.g. UserIDs) are not reissued for use
Wireless Access	Wireless access is authorized, users and computing devices authenticated, and wireless traffic encrypted