viewpoint

Client Security Statement

Version: 4.00

Last Modified: 25 November 2021

viewpoint
redefining governance solutions

Contents

Introduction 3
Information Security Policies 4
Security Policies 4
Security Organisation 5
Access Control Policy 6
User Identity Management 6
Access Management 6
Key Management 7
Antivirus Policy 8
Antivirus Software 8
Software Control 8
Application and Software Security 9
Change Management 9
Security Testing 9
Data Backup and Recovery 10
Physical and Environmental Security 11
Physical Security 11
Perimeter Network Security 11
Cloud Infrastructure 12
Enhanced System Configurations 12
Data Security 13
Data Leakage Protection 13
Data Retention 13
Clear Desk and Clear Screen 13
Disposal of Media 13
Communication and Operational Security 15
Network Controls and Security of Network Services 15
Capacity Management and System Acceptance 15
Information Transfer 15

Asset Management 16

Technical Vulnerability Management 17

- Vulnerability Management 17
- Patch Management 17

Business Continuity Management 18

Security Incident Management 19

- Data Breach Management 19

Logging, Compliance and Audit 20

- Logging 20
- Internal Audit 20
- External Audit 20

Human Resource 21

- Employee Code of Conduct 21

Introduction

The management of Viewpoint takes the security of its information assets and clients' assets very seriously. With the establishment of Information Security Management System (ISMS), its commitment to corporate security is shown through the implementation of policies, controls and procedures, as well as the allocation of dedicated resources required for a formal corporate security organisation.

While information security measurement will naturally change over time and may differ across the range of Viewpoint's services, this overview of the security controls employed by Viewpoint should answer many of your questions regarding our security practices.

This document is intended to be shared with Viewpoint's clients, prospects and suppliers.

Information Security Policies

Security Policies

Viewpoint maintains a comprehensive set of information security and cybersecurity policies and procedures which align with ISO/IEC 27001 standard. It is the policy of Viewpoint to ensure that:

- The reputation of Viewpoint is maintained
- Confidentiality, Integrity and Availability of all Information Assets (owned or handled on behalf of its clients) is maintained
- Information falling under the purview of the scope of the ISMS is protected against unauthorised access, both internal as well as external
- Information will not be disclosed to unauthorised parties
- Allocation of Information Security roles and responsibilities as laid down in the ISMS Policy Statement shall be documented in the job description
- Information Security education and training shall be imparted to all the employees and relevant third-party employees falling under the scope
- Information is available to authorised parties when needed
- Security of networks is maintained by implementing controls to safeguard the network from malicious software and other attacks (internal and external)
- Security of premises is maintained by implementing controls to safeguard the premises from unauthorised access (internal and external)
- Compliance to regulatory, legislative and contractual requirements is ensured according to the laws of the state, country and business
- Integrity of information will be maintained through protection from unauthorised modification
- All kinds of Intellectual Property Right (IPR) is protected
- All suspected breaches of Information Security will be reported, investigated and logged
- Business continuity plans are maintained, reviewed and tested as far as practicable
- Continuous improvement of its Information Security Management System is carried out building greater trust and assurance amongst employees and clients

Security Organisation

Viewpoint has a formal security organisation led by the Information Security Management Representative (ISMR), who is responsible for the security matters in the organisation. ISMR reports to the Viewpoint top management, which has the ultimate responsibility for the organisation security-related decisions and strategies.

Both Information Security and Internal Audit teams assist ISMR for all security governance, compliance and audit activities. HR & Administration, Infrastructure, Compliance, Software Development, Sales and Support Services, Solutions and Project Management are the key security committees under the Viewpoint Security Organisation.

Access Control Policy

User Identity Management

Viewpoint performs background screening on all the employees and security assessment on vendors. The organisation engages a third-party background screening service provider to conduct background investigation. Employee identity is subsequently verified at the initiation of employment via standard human resources processes.

Upon joining, the new hire is required to sign a non-disclosure and confidentiality agreements and employee identification card is issued.

Employees are prohibited from sharing their individual credential, such as username and password. In addition, the corporate email account is strictly not for personal use.

Viewpoint maintains a formal termination or change of employment process to ensure that upon termination or change of employment, all Viewpoint assets are returned, access rights are revoked, user accounts are disabled and former employee will be reminded of restrictions.

Access Management

Strong password controls are enforced when possible, for example, via Active Directory policy settings. The organisation's password standard requires:

- Password change at first login
- A minimum password length
- Password to contain special character, letters and numbers
- Password to be changed regularly
- Deactivation of user account after a number of unsuccessful login attempts

Multi-factor authentication implementation is in place for high-risk cloud-based accounts.

Client data is maintained in production repositories, which resides in cloud environment with multi-factor authentication in place.

Employee access to internet and websites is restricted based on regulatory, information security and internal control requirements.

Key Management

Provide the guidance on the phases of a key life cycle and define a key management solution should operate during these phases. The key management has segregated the roles and responsibilities to different user groups so no one person has full control over the platform. The policy is designed to protect the keys from unauthorised access, unintentional modification, or misuse of the sensitive information. An authentication is needed to perform any operations with the Key Management.

Antivirus Policy

Antivirus Software

All the servers and workstations in Viewpoint are installed with anti-virus program. The anti-virus program is up to date with latest signature file. When the anti-virus scanning detected malicious file from the end user devices, it will alert the Viewpoint Infrastructure Team.

Email filtering is enabled at email gateway to reduce the amount of malware. Viewpoint also utilises a protection system designed to block spam, phishing and viruses from reaching employees' inboxes.

Software Control

An approved software list is maintained, and Viewpoint keeps track of software installed on employees' machines. Any unauthorised software found will be investigated.

Application and Software Security

Change Management

Viewpoint has a formal Change Management procedure complying with ISO/IEC 20000 standard. Secure Software Development Life Cycle is defined to ensure information security is designed and implemented.

To produce a secure software, Viewpoint implements the following practices:

- Design reviews and pre-project planning
- Standard coding guideline and secure coding checklist. Ensure application input parameters are validated and there is proper error handling
- Code-level security reviews with professionally trained peers for all new and significantly modification applications
- Threat modelling and code analysis
- Database integrity validation and review

Security Testing

Viewpoint performs simulated attacks on applications to evaluate the security level of the application.

The penetration testing methodology used by Viewpoint internally and the vendors engaged by Viewpoint is based on several published industry guidelines such as NIST and the Open Web Application Security Project (OWASP) Testing Guide. The approach combines manual and automated assessment techniques and the use of premier proprietary, commercial and open source assessment tools in a consistent and repeatable process. The methodologies cover the following activities:

- Pre-test preparation with application owners
- Automated dynamic/static scans and output verification of scans
- Vulnerability identification and confirmation testing
- Report preparation and delivery with manager review
- Present and discuss findings with application owners
- Issues remediation and follow-up

Data Backup and Recovery

The organisation's backup and recovery are performed according to defined internal procedure outlined in Viewpoint Backup Plan, Business Continuity Management and Viewpoint Backup Recovery Testing Plan.

Backups are written to a separate disk space for recovery purposes. Restoration testing is conducted periodically, and restoration success matrices are maintained.

Recovery efficiency is validated through the breadth and frequency of data restores performed in the course of normal business operations.

Physical and Environmental Security

Physical Security

Viewpoint has standardised physical security measures in its offices, including carded access, video surveillance and visitor management. Access to all facilities is controlled by electronic key systems. Employees are educated about good practices to ensure physical security.

All visitors must register with photo identification and have a confirmed host before being granted access to the offices. Visitor logs are maintained with logbook in reception area. In addition, a special tag is always provided to the visitor with escorting by employee.

Viewpoint facilities are protected from environmental hazards and power outages by the following controls:

- Uninterruptible Power Supply (UPS)
- Air conditioning units
- Smoke detector
- 24 x 7 guard house as well as internal and external CCTV monitoring
- Physically secured network equipment areas and locked cabinets
- Motion detector

Viewpoint Data Centre access is limited to authorised personnel. Visitor access procedures and loading dock security protocols are established.

Perimeter Network Security

Viewpoint resources are built through a tiered network architecture comprising of multiple secure zones to create a highly segmented environment consistent with the defence-in-depth strategy. Secure zones are implemented via a combination of firewalls and virtual local area networks.

Wireless communications are encrypted and isolated, unable to connect with any server and only provide the access to internet. Public wireless access to the Internet is separated and is not connected to the organisation's network.

Cloud Infrastructure

Cloud-based solutions must satisfy the organisation's Cloud control requirements including the encryption of data at rest and in transit, firm-controlled authentication, centralised logging and auditing.

Cloud control requirements:

- Compliance - Offers industry-specific standards and supporting materials for key regulations, for example, ISO/IEC 27001 etc
- Physical Security - Controls are in place to reduce the risk of unauthorised physical access to the data centre resources
- Identity and User Access Management– Multifactor authentication and least-privileged access control to manage user access of enterprise environment, data and applications
- Network Security - Encryption is enabled over the wire for infrastructure communications between VMs to data centre
- Data Protection – Data is encrypted both in transit and data at rest
- Threat Protection – Security alert is enabled to detect anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases
- Log Management – Logs are centralised and monitored
- High Availability – Provide at least 99% of availability
- Disaster Recovery – Threats and risks are identified and classified. Reconstitution mechanism to get the business back to normal from the disaster recovery is planned and simulated half yearly
- Backup – Data is backup followed by backup plan

Enhanced System Configurations

Encryption on organisation-provided laptops is a must for employees who carry sensitive information. This is done using industry standard encryption software.

An inactive screen lock is enforced by a configuration policy on every endpoint.

Data Security

Data Leakage Protection

When handling sensitive information or client related project, a dedicated team with dedicated machines are assigned for the necessary work throughout the project cycle. All the data will be disposed upon project completion.

The team shall comply with the Client Data Handling process to protect the rights and freedom of data subjects and process their data securely by following legal obligations.

Data Retention

Viewpoint retains records for various periods as needed to comply with applicable laws and regulations and to conform to its internal retention policies.

Clear Desk and Clear Screen

Viewpoint ensures that unattended workstations and other work areas are kept clear of papers and other storage media. At the end of each working day, Viewpoint employees keep everything appropriately in a safe or in locked cabinets especially printed reports with 'Restricted' up to 'Highly Confidential' classification.

Computer screens are kept clear of sensitive information when unattended. The screen will be locked after 15 minutes of inactivity and require user authentication to unlock.

Viewpoint Information Security team constantly carries out clear desk and clear screen inspection after office hours or during lunch hour to ensure the employees adhere to the policy.

Disposal of Media

Under both Disposal of Confidential Media and Equipment Security guidelines, all physical hard copies containing sensitive data will be shredded prior to disposal. Removable media will be physically destroyed prior to disposal at its end of life. Hard disks taken out of service for replacement or surplus will be either 'scrubbed' or physically destroyed.

The disposal and destruction of confidential data in the cloud shall go through a proper process, perform and monitor by relevant parties. After the data is removed, the Cloud Service Provider follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware.

Communication and Operational Security

Communication links make up the arterial system of Viewpoint network on which the data and information transfer takes place. Since most of the risks and threats arise from the networked machines only and propagate through the communications links, hence it is required that adequate operational procedures and controls secure Viewpoint's communication links.

Network Controls and Security of Network Services

Viewpoint ensures the information in networks and its supporting information processing facilities are well-protected. All the responsibilities for operating and managing the network and network facilities are clearly defined and documented under the Network Administration Guidelines.

Capacity Management and System Acceptance

Both the Capacity Management Procedure and System Acceptance Procedure are in place to ensure that the use of resources is monitored and tuned. Forecasting on future capacity requirements is implemented to ensure the required system performance is not compromised. System acceptance testing is conducted for the new system, hardware and software, and as specified from time to time.

Information Transfer

Exchange of Information Guidelines describes the proper handling of information transferred within Viewpoint and with any external entity, including our clients and suppliers. This ensures information transfer via conversation, telephone, fax, mobile phones, and electronic messaging are appropriately protected from unauthorised access.

Asset Management

Viewpoint maintains asset information for physical and information assets in managed inventories. Each asset has an owner and a set of attributes to manage the risks and asset lifecycle. The organisation's Information Security policies define a multi-tier scheme for classifying its assets, which are

- Asset classification labelling and handling
- Identification of the information owner and its acceptable use
- Identification and evaluation of security risks
- Implementation of the risk treatment plan

Obsolete assets will be disposed by the centralised Infrastructure team accordingly. Parts that can be reused will be kept and parts that cannot be reused will be scrapped and disposed. Asset Disposal Form will be filled to ensure the asset is properly disposed.

Technical Vulnerability Management

Vulnerability Management

Viewpoint has a comprehensive vulnerability management. A vulnerability scan is performed as scheduled. Vulnerabilities are resolved on a risk-adjusted basis with those that are classified as high-risk immediately remediated. Vulnerabilities are tracked until resolved.

Penetration testing on software and production environments are performed yearly by reputable third-party security firm.

Proper treatments are carried out for discovered vulnerabilities. These vulnerabilities are given a risk-ranked profile with remediation and timeframe.

All penetration testing is done using guidelines from OWASP.

Patch Management

Viewpoint has patch management processes and tools to assess and deploy operating system patches and updates. These patches are tested in a test bed and evaluated before being applied, while risks associated with applying the patches are taken into consideration.

Business Continuity Management

Viewpoint constantly conducts a business impact analysis to identify and establish the changing business needs and technological upgrades. Business Continuity Plan (BCP) is created to counteract disruptions to business activities from failures or disasters due to any uneventful happening and to continue the critical business operations through any eventuality.

BCP is driven by the business needs. It is tested and updated regularly to ensure the plan is up to date and effective. Members of Business Continuity Team (BCT) are appointed to respond and counteract the disaster causing the disruption in IT operations to bring them back to the level of normalcy.

Security Incident Management

Viewpoint has a dedicated Information Security Incident Response Team (ISIRT) that is directly responsible for information security incidents that will cause or have caused an impact on Viewpoint's information systems, information resources, operations or members.

The ISIRT is led by Viewpoint's ISMR and includes staff members from the IT team specialised in particular subjects such as Operating Systems, Networking, Database, etc. The ISIRT may also comprise personnel from other departments.

The entire Security Incident Management procedure includes the early stage from when an incident is reported, incident analysis, containment, escalation and notification, eradication and recovery, and finally lesson learnt.

Data Breach Management

In the event where data is breached, this process outlines the actions to be taken in the shortest timeframe to minimise the harm to the affected parties. The process contains the flow of reporting, containment, assess, notify and evaluate.

Logging, Compliance and Audit

Logging

Security event logging is enabled for all information technology resources and network accesses to allow system forensic analysis. Abnormal pattern and unauthorised access attempts are monitored via the event logs.

Security event logs are protected from unauthorised access, modification and accidental or deliberate overwriting.

Internal Audit

Viewpoint has constituted an internal auditor team. They assess the organisation's overall control environment according to ISMS requirements and controls, raise awareness of control risk, communicate and report on the effectiveness of the organisation's governance, risk management and controls that mitigate current and evolving risks, and monitors the implementation of management's control measures.

Internal auditor team periodically audit the ISMS Implementation at Viewpoint and evaluate it against the industry best practices to ensure that the security setup at Viewpoint is up to date. The audit flow follows a formal process, for example, annual audit plan and internal audit procedure.

External Audit

The external audit is conducted on a yearly basis to ensure Viewpoint complies with ISO/IEC 27001.

Human Resource

Employee Code of Conduct

The Employee Code of Conduct outlines our expectations regarding employees' behaviour towards their clients, vendors, colleagues, supervisors, and overall organisation. It also provides guidance to Viewpoint staff in its decision-making process and actions, and is supported by additional policies and procedures governing the activities of Viewpoint.

Non-compliance with the provisions of the Employee Code of Conduct may lead to internal disciplinary measures.