INFORMATION SECURITY

verita

A Briefing on the Information and Cybersecurity Controls at Verita

Information is critical to our clients and remains a key focus for Verita. The security of data is of the utmost importance, and we continually make sizable investments designed to protect our information and IT assets.

Verita has developed a comprehensive global information and cybersecurity framework aligned to National Institute of Standards and Technology (NIST) frameworks, ISO 27001 and ISO 27002.

Our framework and its underlying controls are designed to ensure that:

- Verita information and systems are only available to authorized people with a justified business need;
- Verita information is not disclosed or modified without authorization;
- Verita information is available when required by relevant business processes;
- applicable regulatory, legislative and client requirements are met;
- information security training is available to all employees;
- breaches of security and suspected weaknesses are reported, investigated, documented and resolved;
- employees have access to relevant additional standards and guidelines that support this policy; and
- our brand and financial resources are otherwise protected from the damage that information security breaches can cause.

This document provides an overview of our information and cybersecurity framework that is in place across our businesses.

Information Security Policies

Verita has an Information Security Policy Framework (ISPF) that is aligned to NIST frameworks, ISO 27001 and ISO 27002 and applies to Verita's business units in all geographic locations. It is owned by the Chief Information Officer, reviewed by key stakeholders across the organization and approved by the Chief Executive Officer.

The ISPF is the collective term for our Information Security Policy Framework. This includes related policies, standards, guides and other associated documents. It is reviewed on a regular basis to reflect any significant changes in Verita's structure, business functions and the regulatory environment, or in response to new and emerging threats. The ISPF is communicated to all employees through training and applicable documentation.

Organization of Information Security

Verita has established an effective, forward-looking information security operating model that is supported by a strong professional capability across the organization.

The Chief Information Officer leads the Information Security Team, providing oversight and guidance on the overall development and implementation of information security across the business. This team works in conjunction with Verita's business units and other support functions including legal, cybersecurity, compliance and technology.

All Verita employees, and certain consultants, contractors and business partners, have their information security responsibilities clearly defined. Specific responsibilities are also included for managers, information owners, information custodians and business leadership.

Human Resource Security

All newly-hired employees are subject to screening prior to employment. The screening processes are conducted in accordance with relevant national laws and industry regulations, and provide verification of identity and credentials, as well as evaluating applicant integrity.

Verita employees are subject to confidentiality/non-disclosure agreements as part of their standard employment and are required to comply with the security controls and associated standards that cover the core safeguarding of Verita information.

Training is provided so that all employees are aware of their responsibilities and possess the necessary resources to maintain our position on information security. This program includes mandatory annual on-line training for all employees, additional trainings that are commensurate with specific job roles and more detailed technical security training for the Verita technology teams.

When an employee leaves, Verita enforces robust procedures to ensure the timely removal of access rights to Verita's IT systems as well as the retrieval of physical information assets recorded in the asset inventories.

Asset Management

Verita has implemented an information classification scheme for all information that supports its day-to-day business activities.

Verita maintains inventories of its information assets, including applications and IT systems. Owners are assigned to all business applications and are required to complete information security risk assessments. This classifies the application based upon business criticality and identifies the required controls to protect the confidentiality, integrity and availability of the application throughout its life cycle in accordance with the classification.

At the end of the information life cycle, all information is securely destroyed prior to reuse or disposal of the information asset.

Access Control

Verita operates on the principle of 'least privilege' for access control. This is to ensure that (i) only authorized individuals are permitted access to our business applications, systems, networks and computing devices; (ii) individual accountability is established; and (iii) authorized users are provided with the access permissions that are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

Our authentication and authorization mechanisms and processes are commensurate with the criticality of the IT system. Access is coordinated through the IT Service Desks and all access requests must be authorized by an employee's manager and/or the assigned resource owner. The Information Security team regularly performs certification reviews of user access rights to detect and remove any inactive accounts and inappropriate access permissions.

All Verita employees are assigned unique user IDs and are required to select and manage their passwords in line with Verita policies. In the event of a change of employment status or role, user access rights are promptly revoked or reassigned by the IT Service Desk upon notification from the line manager.

The use of privileged accounts is strictly controlled and restricted to system administration and maintenance activities only. Additional measures are employed to securely manage these accounts.

This includes enhanced password management controls and more frequent certification reviews.

Cryptography

Verita has incorporated cryptographic guidance with the objective of protecting the confidentiality of Verita information. This includes, but is not limited to, how the information is to be protected within applications, and how to conduct key life cycle management.

Verita utilizes cryptographic solutions to protect data in transit and at rest. Network and wireless networks use industry-recognized leading practices to implement strong encryption for authentication and transmission, commensurate with the sensitivity of the data being transmitted. Mobile computing devices such as smartphones and laptops are encrypted.

Physical and Environmental Security

All Verita office locations operate risk based controls to afford protection against unauthorized physical access. These can include physical and electronic access control systems, manned reception desks, CCTV and security lighting. Access to our critical information processing locations is strictly controlled and restricted to pre-authorized individuals only. This access is logged and the access rights are reviewed on a regular basis.

Data center facilities are designed to be protected against fire, flood, environmental and other natural hazards. Our environmental controls can include fire detection and prevention, dual power supplies, monitored uninterruptable power supply, back-up generators as well as cooling, heating and other infrastructure controls.

Operations Security

Verita has implemented a defense-in depth approach to protect its information and IT systems from existing and emerging threats. The management and operation of our IT systems is delivered by our highly experienced technology teams using a service management model. This includes the formalization of processes and procedures to support core activities such as back-up and recovery, change management, release management and capacity planning.

The approach includes, where required, security architecture principles (i.e., defense-in-depth, least privilege, default deny and fail secure) and the provision of security hardening requirements.

The information security team actively monitors the internal and external threat environment and works with the technology teams to ensure that the current security controls deployed are both appropriate and effective, to mitigate risk.

Resiliency and Monitoring

Verita's secure environment provides comprehensive disaster recovery and resiliency features to ensure business continuity and data protection. Utilizing features such as secure backup, site recover and distribution of services across multiple geographic locations to safeguard against regional and other failures, Verita is able to maintain high availability, minimize downtime and ensure data integrity during unexpected events.

The Verita IT network is monitored 24x7. Event logs from network devices, firewalls, intrusion detection systems and web application firewalls are collected and analyzed; and any unusual or suspicious events generate the necessary alerts which are handled in accordance with our information security incident management processes.

System Acquisition, Development and Maintenance

Verita has a wealth of in-house experience in delivering best-in-class business applications and IT systems. We follow a defined life cycle that incorporates information security throughout each stage including risk assessments, the identification and implementation of control requirements, static and dynamic code analysis and technical security penetration testing based on a risk assessment.

Verita maintains separate development, test and production environments and has strict policies to enforce segregation of duties for employees responsible for development, testing and support activities. Our source code, including all applications under development, are stored and protected in an approved source code system with audit logging enabled to track activity such as code modification and deletion.

Our business applications and IT systems classified as critical by the information security risk assessment process have enhanced information security controls.

Supplier Relationships

Verita operates a vendor management program to identify, assess and manage information security requirements that are contractually agreed with certain authorized third-party suppliers that access, store, process or transmit information on our behalf.

Information Security Incident Management

Verita has risk-based processes to respond to information security incidents, unusual or suspicious events and breaches of policies.

These processes are owned and coordinated by the information security team with formal involvement from relevant stakeholders (e.g., risk, legal, compliance, technology, human resources, internal communications, the financial crime team and public relations).

The information security incident management processes are designed to contain and control the incident, reduce any potential impact to the business, identify and investigate the root cause and implement corrective actions to reduce the risk of recurrence. These processes are supported by procedures for identification, reporting, assessment, response, recovery and follow-up. Our post-incident procedures include root cause analysis, forensic investigation and, where required, notification to the relevant authorities and affected clients.

All Verita employees are provided with training and guidance to identify and report information security incidents. The individuals responsible for managing information security incidents are supported by more specific training and access to relevant tools to complete each stage of the information security incident management process.

Information Security Aspects of Business Continuity Management

Verita has an established business continuity management program that supports our regulatory and contractual requirements.

Verita business units are included within the program and are required to complete a risk assessment and business impact analysis with the resulting creation of a business continuity plan. This provides a consistent methodology to define the recovery time objectives incorporated into specific business continuity plans.

Our business continuity plans and disaster recovery plans are developed and maintained by assigned owners from the business and technology teams and are regularly updated to reflect any change of circumstances.

Verita performs business continuity and disaster recovery tests on a periodic basis to ensure that the plans can be employed should the need arise.

The test results are communicated to our senior executive management and relevant stakeholders upon completion.

Compliance

Verita has an established governance, risk and compliance model that is endorsed by our executive management. The information security team measures compliance with the Information Security Policy and underpinning standards through periodic technical and non technical control assessments. Our technical control assessments include system patch verification, application and infrastructure vulnerability scans and penetration tests.

Summary

We trust this demonstrates the ongoing commitment and considerable investment Verita continues to make in information and cybersecurity and that our clients, business partners, employees and shareholders can have full confidence in the confidentiality, integrity and availability of our information and IT systems.

This document is intended to provide an overview of Verita's information security controls for informational purposes only.

If you have any specific questions or would like additional information on the measures that we take to protect your information, then please contact your Verita relationship manager.

Information in this document is subject to change without notice.