VERITAS

Provider Security Requirements

[Last updated: 30 September 2021]

A. Veritas Security and Architecture Requirements

The service provider (or “Provider”) shall operate in compliance with the requirements set forth in this Provider Security Requirements document.

Nothing herein is intended or shall be construed to limit Provider’s obligations to Veritas under any agreement, statement of work or other terms or conditions (collectively “Agreement”) between Veritas and Provider. In the event of any conflict between such provisions and this Provider Security Requirements document, the stricter, higher or more protective standard shall govern unless otherwise expressly agreed to in writing and signed by both parties.

B. Definitions

TERM	DEFINITION
Veritas Data	Any Veritas data, including but not limited to data provided to Veritas by third parties that Provider is provided with, or has access to, pursuant to the applicable Agreement with Veritas. Such data may include but is not limited to Veritas source code.
Data Protection Legislation	All applicable national data protection and privacy legislation in force from time to time; all applicable data protection and privacy legislation in force from time to time in the European Economic Area (“EEA”), Switzerland, the UK and the United States of America including, but not limited to, the General Data Protection Regulation (EU) 2016/679) (“GDPR”), the Data Protection Act 2018, California Consumer Privacy Act of 2018, codified at Cal. Civ. Code §1798.100 et seq and any other applicable legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (as defined by Data Protection Legislation).
Handle (or “handle”)	When Veritas Data (in any form and on all types of media) is transmitted through or placed on any Provider resources to perform contracted services.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data whose processing is subject to the Data Protection Legislation.
Provider Resources	Provider resources means any equipment, device, technology, software, software images, access, content or property owned or controlled by Provider or any third party engaged by Provider or acting on Provider’s behalf including but not limited to its agents, contractors and subcontractors. Examples of Provider resources include but are not limited to: • Computing Systems (computers and laptops) • Software and software images • Electronic Messaging (Outlook, Teams, Messenger) • Telephony and Cellular Phone Usage • Mobile Devices • Internet Usage • Applications or intranet usage

TERM	DEFINITION
Veritas Resources	Veritas resources means any equipment, device, technology, software, software images, access, content or property provided to Provider by or on behalf of Veritas, including all information, materials, data, technology, software, applications and source code contained therein. Examples include, but are not limited to: • Veritas Computing Systems (computers and laptops) • Software and software images • Electronic Messaging (Outlook, Teams, Messenger) • Telephony and Cellular Phone Usage • Mobile Devices • Internet Usage • Applications or internal networks (e.g. Oracle, VPN)

C. Evidence of Compliance

1. Third Party Security Audit

Provider shall provide, maintain and renew an independent, third party audit which attests to the effectiveness of controls covering, but not limited to, the requirements defined below in *Section D Security*. Upon request, Provider shall provide such certification or audit results to Veritas.

Veritas will accept (i) an ISO/IEC 27001 certificate with its Statement of Applicability (SOA) or (ii) a SOC 2, Type 2 third-party audit report that covers all locations where Veritas Data is handled, transmitted or stored.

Provider shall provide Veritas with this initial evidence of compliance within thirty (30) days from the effective date of the relevant Agreement between Veritas and Provider and annually thereafter, at Provider's own expense. For clarity, (i) Provider must also provide the required evidence for each of its affiliates, subcontractors and other third parties that handle Veritas Data for or on behalf of Provider, if any, and (ii) the requirements in this Section C.1 do not apply to any Veritas Resources that Provider may be using.

2. Executive Summary of Network & Application Penetration Tests

Provider shall provide the executive summary portion of a third-party penetration test related to the portion of their network and applications that connect to any Veritas network or that access, process, or store Veritas Data. The penetration test shall be performed by a Global Information Assurance Certified (GIAC), an Information Assurance Certification Review Board (IACRB) certified or similarly certified practitioner.

The third-party network penetration test shall be done at least annually and after significant changes have been made to the network. All critical vulnerabilities as defined by industry standards (e.g., Common Vulnerabilities Scoring System (CVSS)) shall be remediated within thirty (30) days of initial identification or identified as a residual risk where action(s) should be taken to remediate as soon as possible.

Provider shall provide Veritas with this initial evidence of compliance within thirty (30) days from the effective date of the relevant Agreement between Veritas and Provider, and upon request thereafter. For clarity, (i) Provider must also provide the required evidence for each of its affiliates, subcontractors and other third parties that connect directly to the Veritas network and/or handle Veritas Data for or on behalf of Provider, if any, and (ii) the requirements in this Section C.2 do not apply to any Veritas Resources that Provider may be using.

3. Vulnerability Scan

Providers that host internet accessible sites on behalf of Veritas (either directly or through third parties) shall scan all such sites before going live, at least annually thereafter and at any time a major change is made to a hosted site that could introduce vulnerabilities (i.e., hardware updates, and other changes as set forth in Provider's change management policy.

Provider shall submit to Veritas a scan report showing that all critical web vulnerabilities are remediated. Provider shall obtain express written approval via email from a Veritas Global Security Office representative

BEFORE any hosted site can go-live or be made publicly accessible. Provider shall submit to Veritas subsequent reports for each website upon request thereafter.

4. Service Provider Attestation of Compliance

Veritas is a Payment Card Industry (PCI) Level 4 merchant. Providers that process, store or transmit card holder data on behalf of Veritas shall be compliant with the then-most current version of the PCI Data Security Standards (DSS) applicable to a PCI Level 4 Service Provider. Provider shall provide a Service Provider Attestation of Compliance (AOC), a Self-assessment Questionnaire (SAQ) and a quarterly network scan completed by an approved scanning vendor showing PCI Level 4 compliance for the Provider itself and any third party engaged by Provider or acting on Provider's behalf to process, store or transmit card holder data.

Provider shall provide Veritas with this initial evidence of compliance within thirty (30) days from the effective date of the relevant Agreement between Veritas and Provider and annually thereafter. If at any point in time, Provider becomes aware that their environment has become non-compliant with the current DSS, Provider shall disclose to Veritas the nature of the control failure within ten (10) business days of discovery.

5. Business Continuity and Disaster Recovery

Providers that host SaaS applications/internet accessible sites used by Veritas where Veritas Data is collected, processed, stored, transferred, destroyed after no longer required, shall provide annually a Business Continuity Plan/Disaster Recovery Program (BCP/DRP) that includes:

a. A business impact analysis describing risk factors associated to Provider's business and service.
b. Provider shall complete and provide BCP/DR testing results at least annually. Veritas shall be allowed to participate in BCP/DR test exercises.
c. Veritas shall be able to obtain BCP/DR test reports, summaries and or documents of BCP/DR program and applicable regulations.
d. Published Recovery Point Objective (RPO) and Recovery Time Objective (RTO) in hours for the service.
e. Explain conditions/penalties when BCP/DR process fails to meet resiliency and availability requirements. For example, what process steps does the provider perform when unable to meet RPO and RTO objectives?
f. "Provider shall follow Data Breach Notification Requirements" (Section D.7) regarding unlawful disclosure of Veritas Data.
g. Veritas shall have a Right to Audit the Provider's BCP/DR program.
h. If the above services are subcontracted by the Provider, then the subcontractor(s) will be governed by the same requirements as the primary.

D. Security

1. All-Level Requirements

a. Providers that connect directly to the Veritas network and/or handle Veritas Data will ensure that Veritas Data will be stored, processed, and transmitted only on a network or system covered under such certification or audit, i.e., SOC 2 Type 2 and/or ISO 27001; and will provide such certification or audit at their own expense.
b. Provider shall provide annual security awareness training to all personnel supporting the Veritas account. Security Awareness training shall address security topics to educate users about the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms. Training materials shall be reviewed and updated at least annually. Training materials should address industry standard topics which include, but are not limited to:
    - The importance of information security, the consequences of information security failures and how to report a security breach.
    - Physical controls such as visitor protocols, safeguarding portable devices and proper data destruction.
    - Logical controls related to strong password selection/best practices.
    - How to recognize social engineering attacks such as phishing.
    - Unique security controls and or requirements placed on the line of business by Veritas.
c. Providers that develop or deliver source code to Veritas or that handle any Veritas source code (including without limit any Veritas product or service source code) shall provide annual secure code training to all personnel supporting the Veritas account. Developers shall be proficient in the OWASP Top 10 and/or the CWE/SANS Top 25 vulnerabilities and their appropriate remediation techniques.

d. Provider shall ensure that the system (Network, Hosting and Application) is designed in compliance with the least privilege principle. Least Privilege refers to the security objective of granting users only those accesses they need to perform their official duties (Refer to NIST SP800-14).

e. Provider shall ensure that the separation of duty principle is rigorously applied. Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process.

f. Provider shall enforce the use of strong passwords for all systems (Network, Hosting, and Application). Strong password is defined as a minimum length of eight (8) characters, inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID that is changed at least every ninety (90) days. Provider shall ensure that username and password are never sent in clear text format and are not shared amongst users.

g. Provider shall ensure that access to the system (Network, Hosting and Application) is logged.

h. Provider shall retain all log files for at least six (6) months and access to these log files is restricted to authorized personnel only.

i. For administrative accounts, Provider shall use two-factor authentication (multi factor authentication for highly privileged administrators) or other positive controls such as increased password length, shorter password life or restrictive white lists of users to restrict access to administrative accounts.

j. Provider shall implement effective user termination / transfer controls that include access removal / disablement immediately upon termination or transfer of staff.

k. Provider shall review access privileges at least quarterly and adjust access privileges in support of the need-to-know and least-access privileges principles.

l. Documented change control process will be used to record and approve all significant changes to Provider's environment.

m. Provider shall implement operating system hardening for hosts/infrastructure handling Veritas Data and/or Veritas Data. Operating system hardening includes, but is not limited to, the following configurations and practices:

- Strong password authentication
- Inactivity time-out
- Turning off unused ports/services
- Log management
- Disabling or removal of unnecessary or expired accounts
- Changing default account passwords and if possible, default account names
- Timely patching and updates to system software

In addition, Provider shall implement strong access control and restrict access to operating system configurations to authorized, privileged users for hosts/infrastructure handling Veritas products or Veritas Data.

n. Provider shall have a documented patch management program and perform patch management at least quarterly on all systems that handle any Veritas Data. Provider shall implement critical patches within vendor recommended timeframes on all systems that handle Veritas Data, not to exceed thirty (30) days.

o. Provider shall implement specific controls to track and verify activities of users with elevated privileges to systems that handle any Veritas Data, including, but not limited to separation of duties, maintaining log files, maintain security logs for all access to Veritas Data, cameras, etc. Records such as CCTV recordings, entrance logs and other monitoring devices shall be kept a minimum of thirty (30) days.

p. Provider shall maintain a Third-Party Risk Management Program to ensure that security risks presented from vendors, partners, and contractors (Veritas' fourth parties) are identified and remediated for those who are required for the Provider to perform services/provide products to Veritas.

2. Network-Level Requirements

a. Provider shall use firewall(s) to protect hosts/infrastructure handling Veritas Data. The firewall(s) shall be able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing.

b. Provider shall have network-based security monitoring (i.e. syslog, security information and event management (SIEM) software or host-based intrusion detection systems) for the segment(s) which handles Veritas Data.

c. Provider shall assess network-level vulnerabilities through a third-party penetration testing. Refer to *Section C.2 Executive Summary of a Network Penetration Test.*

d. Provider shall employ ongoing, active network scanning to assess potential vulnerabilities, and shall remediate those vulnerabilities within a reasonable time (critical vulnerabilities not to exceed thirty (30 days). All other vulnerabilities to be remediated during scheduled patching cycles).
e. Provider is not permitted to use a Dynamic DNS service for their external facing website IP address. If a static IP address cannot be provided, then a non-Internet-based method of interaction/communication shall be used.

3. Hosting-Level Requirements

a. Where Provider either (i) Handles Veritas Data or (ii) connects to any Veritas network, Provider shall, at a minimum quarterly, assess system-level vulnerabilities and remediate critical vulnerabilities within thirty (30) days.
b. Provider shall employ a comprehensive anti-virus and malware protection solution with daily signature updates for hosts which handle Veritas products or Veritas Data. Provider anti-virus programs shall have the capability to detect, protect, and remove all known malware software.
c. Where Provider either (i) Handles Veritas Data or (ii) connects to any Veritas network, servers shall be protected from unauthorized access with appropriate physical security mechanisms including, but not limited to, badge access control, locked cages, secure perimeter, cameras, monitored alarms, and enforced user provisioning controls (i.e. appropriate authorization of new accounts, timely account terminations and frequent user account reviews).
d. Where Provider either (i) Handles Veritas Data or (ii) connects to any Veritas network, servers used to provide services will be dedicated exclusively to host Veritas data. If no physically segregated environment is available, Provider shall implement and maintain logical controls to prevent data leakage between customers and the external environment.
e. Providers that host internet accessible sites on behalf of Veritas shall employ industry standard scanning tools to identify website vulnerabilities.

4. Application-Level Requirements

a. Provider shall maintain documentation on overall application architecture, process flows, and security features for applications handling Veritas Data.
b. Provider shall employ documented secure programming guidelines and protocols in the development of applications handling Veritas Data. Provider shall be responsible for verifying and maintaining evidence that all members of the developer team have been successfully trained in secure programming techniques.
c. Provider shall have a documented application patch management program and perform patch management on all applications that handle Veritas Data on an at least quarterly basis. Provider must implement critical patches within vendor recommended timeframes on all applications that host or handle Veritas Data.
d. Provider shall have a documented program for independent secure code review and maintain documentation of secure code reviews performed for all applications and their changes that handle Veritas Data prior to going live.
e. Provider shall employ industry standard change management standards for all applications handling Veritas Data.
f. Provider must use a threat model methodology to identify the key risks to the important assets and functions provided by the application, conduct an analysis of the most common programming errors, and document in writing that they have been mitigated.
g. Provider shall assess application and system level vulnerabilities and remediate them as described in subsection (4.i) below. For the purposes of this section, vulnerabilities shall be assessed, at minimum, on a quarterly basis, and before go-live or after any change of any service to Veritas and/or go-live of Veritas applications.
h. Provider shall employ industry standard scanning tools to identify application vulnerabilities in application development and testing phases.
i. The Provider shall remediate all vulnerabilities identified prior to production, except for vulnerabilities identified as “low” as reported by the scanning tools which may be fixed subsequent to go-live. For applications developed for Veritas, the Provider shall provide recent scans to Veritas on demand in a secure manner.
j. Provider shall adhere to secure deployment practices. Provider shall ensure that deployed applications are not running as root/administrator, but rather as user level or service level with restricted privileges.

5. Data-Level Requirements

a. Provider shall use NIST approved encryption standards (e.g. SSH, TLS v1.2 or higher) for transmission of Veritas Data and Provider shall use NIST approved encryption or hashing standards for storage of Highly Confidential Data.

b. If Veritas Data is stored on a third-party laptop, that laptop shall be protected by full disk encryption.

c. Data and media shall be destroyed at Veritas' request.

d. Provider shall ensure that access to all Veritas Data, including but not limited to information and application system functions, architecture documentation, vulnerability reports and Veritas Data, including source code, is restricted to authorized personnel only.

e. Veritas Data shall not be shared with any other third party under any condition unless pre-approved in writing by Veritas' Legal department on a case-by-case basis.

f. Veritas Data stored on archive or backup systems shall be stored at the same level of security or better than the data stored on operating systems.

6. End User Computing Level Requirements

a. Provider shall employ a comprehensive anti-virus and malware protection solution with daily signature updates and a firewall solution for end user computing devices which connect to the Veritas network or handle Veritas Data.

b. Provider will prohibit and disable the use of non-managed external devices for storing or carrying, or in use with machines handling Veritas Data. Remote devices include without limit: flash drives, CDs, DVD, external hard drives and other mobile devices.

c. Provider shall keep all critical OS-level patches up to date.

d. Provider shall use up to date internet browsers.

e. Provider shall keep all recent critical middleware (i.e. Java, Adobe), browser-related patches up to date.

7. Data Breach Notification Requirements

a. Provider shall notify Veritas immediately within four (4) hours of awareness if a confirmed breach involving Veritas Data. Where there is a Personal Data Breach, Provider shall notify Veritas without undue delay after becoming aware of it. Notifications will be sent to cybersecurity@veritas.com. Provider will update Veritas every four (4) hours regarding the security incident.

b. Provider shall work with Veritas promptly and in good faith as required to resolve the breach or incident, and in conjunction with any associated investigations.

8. Compliance Requirements

a. Notwithstanding any of the foregoing, Provider shall adopt appropriate physical, technical and organizational security measures in accordance with industry standards, including but not limited to building access control, employee security awareness education, etc.

b. Provider will, when and to the extent legally permissible, perform criminal background verification checks on all its employees and third parties that provide services to Veritas prior to obtaining access to Veritas Data. Such background checks shall be carried out in accordance with relevant laws, regulations, and ethics, and shall be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks of customer data loss associated with the Provider's performance of services.

c. Provider will maintain an Information Security Policy (ISP) that is reviewed and approved annually at the executive level. The Provider shall ensure that all employees, contractors, and subcontractors are familiar and comply with the policy. Provider commits to enforcing compliance to the provisions of that ISP, including but not limited to security awareness and good security practices including but not limited to a clean desk policy; locking screens; account lockouts after multiple failed login attempts; not sharing passwords; not keeping physical copies of passwords; questioning unknown individuals on premises.

d. Provider shall comply with all applicable regional and global regulatory requirements including but not limited to the Data Protection Legislation, Sarbanes-Oxley (SOX), PCI etc., as they apply to the Provider's environment supporting the service being provided to Veritas.

e. Provider shall implement and maintain technical and organizational security controls to protect Veritas Personal Data from unauthorized or unlawful processing against accidental loss, destruction, damage, theft, alteration or disclosure. The provider will acknowledge this requirement through signing a separate Personal Data Processing Agreement.

9. Supplier Risk Assessment (SRA)

a. In addition to Veritas' inspection and audit rights as set forth in any relevant Agreement, Veritas reserves the right to request a security questionnaire from Provider. If Provider fails to comply with such request within a reasonable timeframe, or if the security questionnaire raises Veritas security concerns that are not addressed by Provider to Veritas' satisfaction, Veritas reserves the right (in addition to any other audit or other rights it may have) to conduct, or engage a reputable third party auditor to conduct an SRA.

b. Where a legal or security breach has occurred, Veritas may conduct an SRA at the Supplier's expense. Provider will provide prompt, full and good faith cooperation in the performance of the SRA.

c. If any findings or problems are identified from the SRA, Provider agrees to remediate all findings in a reasonable, agreed upon timeline.

10. Veritas Resources

a. Providers that use Veritas Resources shall strictly adhere to Veritas' Acceptable Use Requirements in the Asset Management Security Standard. Provider commits to enforce this policy, including but not limited to ensuring all of the following:

   i. Veritas Resources may not be modified in any way
   ii. Veritas Resources will not be used to connect to any non-Veritas network
   iii. Veritas Resources will not be used to provide services to any other party
   iv. All Veritas Resources will be returned to Veritas at the end of the service period, or upon demand
   v. Veritas data will not be removed from Veritas Resources and placed on other end-points or stored on other media or networks

b. Provider's VPN access will be granted on an as-needed basis and shall be approved by Veritas Global Security Office on a case-by-case basis.

11. Physical security

Provider shall have physical and environmental controls that are commensurate to the risk for Veritas' Confidential Information and for the Provider equipment, assets, or facilities used to hold and process such information.

12. Media and Data Destruction

a. Destruction Requirements and Compliance Evidence

1. *Destruction Requirements*. Any and all Veritas Data is and shall remain the sole property of Veritas, and Provider shall not acquire any rights or licenses therein except as expressly set forth in the relevant Agreement. Provider shall return to Veritas (or at Veritas' option, destroy) any and all Veritas Data and any other information and materials that contain such Confidential Data (including all copies in any form) immediately upon Veritas' request, or upon the earlier of the completion of Services or termination of the relevant Agreement.
2. *Certificate of Destruction*. Within ten (10) days following Veritas' request, Provider will provide Veritas with a written certificate of destruction, as signed by an officer or executive level employee of Provider, certifying to Provider's compliance with this Media and Data Destruction Requirements document.