SITA SECURITY REQUIREMENTS FOR THIRD PARTIES

ENTERPRISE INFORMATION SECURITY OFFICE

Version: 1.0
Date Issued: 11/9/2022

1 INTRODUCTION

This document describes SITA's information security requirements of third-party service providers ("Provider") that accesses, process, store or transmit data on behalf of SITA. The requirements set forth in this document should be used by procurement to frame Provider negotiations. Where the Provider cannot, or will not, meet the requirements an alternative provider should be considered.
Where no suitable alternative provider can be found, SITA procurement must document those areas with which the Provider cannot comply and gain formal written approval from EISO prior to signing the contract.

2 REQUIREMENTS

2.1 GENERAL REQUIREMENTS

a) PROVIDER will maintain and follow IT security policies and practices that are integral to PROVIDER's business and mandatory for all PROVIDER employees, including supplemental personnel.

b) PROVIDER will review its IT security policies at least annually and amend such policies as PROVIDER deems reasonable. PROVIDER will notify SITA of any changes to the Provider's security policy.

c) PROVIDER will maintain and follow its standard mandatory employment verification requirements for all new hires, including supplemental employees, and extend such requirements to wholly owned PROVIDER subsidiaries. These requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by PROVIDER.

d) PROVIDER employees will undergo security and privacy training and awareness to ensure they comply with PROVIDER 's security policies, and records of training should be maintained.

e) PROVIDER will ensure that all employees and representatives who will perform work or have access to information resources associated with SITA are covered by binding/signed non-disclosure agreements

f) PROVIDER will ensure that physical PROVIDER related work areas are secure to prevent unauthorized physical access, damage and interference. PROVIDER will restrict and limit access to SITA Data and SITA information systems by defining roles and segregating duties (to avoid conflicts of interest in security activities), establishing authorization processes and by implementing a technical solution that manages the access rights of users from their onboarding to the end of their assignment and access rights. Access rights to SITA Data and information systems will be periodically reviewed

g) Consistent with industry standard practices, and to the extent supported by each component managed by PROVIDER within the Service, PROVIDER will enforce timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, implement dual-factor authentication whenever possible, ensure accesses are uniquely identifying a person and/or a system and maintain sufficient audit records of accesses for at least thirty days. PROVIDER will ensure that authentication mechanisms cannot be overcome.

h) PROVIDER will limit the number of privileged users and will appropriately monitor their access with extensive logging.

i) PROVIDER personnel remotely accessing Systems and data in relation to the Service will be individually identified and authenticated using two-factor authentication, and their login attempts will be monitored.

j) PROVIDER will ensure that the termination process for its employees includes return of, and revoking of access rights to, all SITA information assets.

k) PROVIDER shall maintain logs of all Events on systems and networks used to process Personal Data ("Event Logs"), including information such as date, time, user ID, device accessed, and port used. PROVIDER shall maintain such Event Logs for a minimum period of twelve (12) months. If requested by SITA, PROVIDER shall allow SITA to analyze the Event Logs for security related events, unusual activities and other issues, such as unsuccessful attempts to create backup copies of data. For the purpose of this section, "**Event**" shall mean: any incident that may result in damage to any information security assets, Personal Data, and/or operations of systems and networks.

l) PROVIDER will secure all SITA Data by encrypting the data and/or the link between the two communication ends, using reliable implementations of network protocols and encryption algorithms, in compliance with legal requirements in the country of operation and as recommended by security best practices. PROVIDER will communicate to SITA the secure network protocols and encryption algorithms used.

m) PROVIDER will encrypt SITA stored sensitive data, including personal data, on all information systems deemed sensitive, using reliable encryption algorithms (compliant with FIPS 140-2) in compliance with legal requirements in the country of operation and as recommended by security best practices.

n) PROVIDER will perform or have performed annual penetration testing on all deemed sensitive information systems or upon major service changes, while avoiding operational and business disruption.

o) PROVIDER will implement antimalware solution on all relevant information systems.

p) PROVIDER will subscribe to an external threat intelligence service in order to receive regular timely information of current threats and technical vulnerabilities for all relevant information systems. PROVIDER will build a patch management process based on current best practice

q) PROVIDER will implement Next Generation firewalls with dedicated rulesets/policies that will be periodically reviewed as part as the general security review process. The technologies used will be regularly updated as part of the patch and vulnerability management process.

r) PROVIDER will perform automatic vulnerability scanning, while avoiding operational and business disruption.

s) PROVIDER will assess business impacts and security risks regarding all relevant information systems, at least annually and upon any major change in the operating environment.

t) PROVIDER will implement an effective backup and restore strategy regarding SITA Data and implement reliable technology to support its strategy. Backed up data at rest should be encrypted within its container, data sent between the backup server and the backed-up resources should be encrypted in transit. At least one backup copy should be kept on a remote location, not subject to natural threats (e.g. flood).