SITA Information Security

SITA Security Requirements for Third-Party Service Providers that Access, Process, Store or Transmit Data on Behalf of SITA

September, 2012

Contents

1. Introduction

1.1 Overview

This document describes SITA's information security requirements for third-party service providers that access, process, store or transmit data on behalf of SITA ("**Providers**").

1.2 Scope

These security requirements apply to:

- all systems used by Provider in the course of performing service for SITA or on behalf of SITA ("Systems"); and
- all users associated with the Provider in the course of performing service for SITA or on behalf of SITA ("Users").

2. Requirements

2.1 General Requirements

Provider must:

- indemnify SITA for any, failure to perform, and/or failure to comply with the security requirements contained in this document.
- complete SITA's Information Security Questionnaire and provide to SITA Business Owner for assessment by the Corporate Information Security Office (CISO).
- 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 and non-compete agreements.
- secure and protect SITA proprietary information, SITA employee proprietary information, SITA customer proprietary information, and/or other SITA information resources from unauthorized or improper use, theft, or accidental or unauthorized modification, disclosure or destruction.
- assure the reliability and integrity of all SITA information and information resources under its control, and the information processing activities performed with or for SITA.
- notify SITA of any updates or changes to the Provider's security policy.
- report to SITA, within 24 hours of discovery, any known or suspected unauthorized access, use, misuse, disclosure, destruction, theft, vandalism, modification, or transfer of SITA, SITA employee, and/or SITA customer proprietary information. Reports should be sent via email to the SITA Security Incident Response Team (SIRT@SITA.aero).
- return proprietary information to SITA and completely destroy proprietary information in compliance with legal or regulatory requirements or upon written request from SITA.

Provider may not contract out any obligation herein without prior written approval from SITA.

2.2 Administrative Security

Provider must:

- have a documented Information Security Management System (ISMS). The ISMS should cover all of the requirements of ISO/IEC 27001 and be proven to be operating effectively through periodic internal and/or external audits by independent and qualified practitioners;
- designate a Security Point of Contact within the Provider's organization to act as the Liaison between SITA and the Provider;
- ensure that only individuals with an approved need to know are allowed to access SITA information, SITA employee information, and/or SITA customer proprietary information;
- ensure sufficient separation of duties of Provider personnel to prevent a single individual from committing fraud with, or abusing, SITA systems or data;
- perform an appropriate background check for each employee and/or representative who has access to SITA, SITA employee, and/or SITA customer proprietary information;
- have an "Acceptable Use" policy applicable to, or agreement entered into with, each new hire, and the agreement must address acceptable usage of Systems for email, applications, and web browsing;
- have a data classification system and SITA information must be classified according to its sensitivity and must be classified at least as 'Private';
- ensure that its employees receive security awareness training upon hire and annual refreshing sessions thereafter, and acknowledge participation. Participation reports must be made available for review by SITA upon request;
- have a formal change management program in place that requires formal security validation and approval from the Provider's designated Security Point of Contact for any changes to Systems that could reasonably be deemed to have an impact on the security environment within the Provider organization;
- have an Incident Response Plan and related procedures in place for implementation in the event of a security breach. The plan must be tested at least annually. The documented plan and test results report must be made available to SITA upon request. The plan must include notification of the incident to SITA;
- have audit logging enabled that tracks what an individual User has done and when. Audit logs must be retained for at least one year and must be made available to SITA upon request;
- have Disaster Recovery and Business Continuity management programs in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures and disasters. These programs must be tested at least annually.

2.3 Logical Security

Provider must:

- have an established and effective patch management program and implement security changes, patches and upgrades in Systems, applications and software in a timely manner and commensurate with the threat, as directed by the manufacturer and subject to appropriate testing. Security patches and upgrades correcting significant security issues must be implemented no later than 30 days after their release unless a shorter or longer period is recommended by the manufacturer or agreed to by the Provider's designated Security Point of Contact;

- ensure that the termination process for employees includes return of, and revoking of access rights and mechanisms to, all SITA information assets, applications, hardware, software, network and facilities;
- ensure that individual access and accountability controls are in place for each of Provider's employees and representatives who will access a SITA system, application or other information resource. Accountability/audit records shall be kept for a period of no less than thirty days;
- conduct periodic review of access rights and adjustment of those access rights as necessary;
- ensure that authentication mechanisms cannot be overcome;
- ensure that network connections are designed, implemented and maintained so as to secure and protect information, data, and system operation during the life of the agreement with SITA. This includes, but is not limited to, non-repudiation, authentication, authorization, and monitoring issues;
- require that individuals using remote access to Systems for maintenance and/or administrative purposes shall be individually identified and authenticated by an independent, dedicated, access control device that is a part of a network authentication infrastructure. The remote authentication process must use two-factor authentication;
- ensure that System's login procedures are designed and implemented with a mechanism that will thwart the use of repeated login attempts to guess or otherwise determine a valid login identification and authentication combination;
- have anti-virus software deployed on all systems commonly affected by viruses. All anti-virus programs must be kept current, actively running, generate audit logs, and must be capable of detecting, removing, and protecting against other forms of malicious software (e.g. adware, spyware);
- have an effective monitoring program implemented to proactively alert on suspected breaches;
- have a vulnerability assessment process that includes assessments of Provider's hosts, networks, and applications.

2.4 Physical Security

Provider must:

- secure work areas to prevent unauthorized physical access, damage and interference to business premises and information. This applies to, and is not limited to Systems development, testing, integration, and production environments, as well as backup media, printed reports, and email;
- use appropriate facility access controls to limit and monitor physical access to work areas where the provision of the service detailed in the agreement with SITA are undertaken;
- have emergency procedures in place for addressing physical security breaches and incidents.

2.5 Protected Data

Provider must:

- be PCI DSS compliant if any payment card data is stored, processed, or transmitted, and acknowledge in writing that Provider is responsible for the security of cardholder data. (Note: PCI DSS means the Payment Card Industry Data Security Standard, defined by the Payment Card Industry Security Standards Council);
- in the event of a security intrusion involving payment card data, provide reasonable business cooperation, and access to any SITA representative and/or any Payment Card Industry representative or Payment Card Industry approved third party for the purposes of conducting a thorough security review;
- not use or transfer SITA, SITA employee, and/or SITA customer information or data for any purpose not explicitly defined and authorized in the agreement with SITA.
- ensure that no individually identifiable customer data shall be transferred to a third party unless specifically authorized by SITA.

2.6 Software Development: General Security

Provider must:

- test all system and/or software security features before delivery to SITA;
- deliver all systems and software with security mechanisms installed and functioning, all default passwords expired, all test data and accounts removed, and all custom application accounts, usernames, and/or passwords removed;
- provide documentation on security setup and administration for system administrators;
- train all developers in secure programming methods. Records of such training must be maintained for SITA audit;
- use secure coding practices that are consistent with OWASP (Open Web Application Security Project) secure coding guidelines;
- complete a security scan of the system and correct all significant vulnerabilities discovered before the system is delivered to SITA and before applications are accepted and payment is rendered;
- provide written documentation to SITA concerning any and all known security flaws in system or software at the time those flaws become known;
- provide security flaw remedies or "fixes" to SITA at no additional cost to SITA. Such “fixes” shall be supplied to SITA in in a timeframe approved by SITA;
- have a change/configuration management system in place that governs the integrity of its systems and software delivered to SITA.

2.7 Software Development: Software Integrity

Provider guarantees that software code created or modified for SITA:

- does not contain any master access key (ID, password, back door, etc.) to the system;
- does not contain computer viruses, worms, or other destructive code;
- does not degrade security by interfering with or modifying the normal functions of the operating system on which the software will reside;
- does not degrade security of any application code or other software;
- will record, store, process and display correct calendar dates.

3. SITA Audit Rights

SITA retains the right to conduct security audits at short notice either remotely or on-site in order to confirm Provider's compliance with the security requirements contained herein.

Audits may be performed by SITA employees or an independent auditing firm.

Audits may include all computer systems, applications, software, files, and records that store data obtained from or resulting from the use of SITA's information resources, or which are used in the performance of work for SITA.

Audits may include, but are not limited to, operating system security, application security, database security, physical security, network security, program change control, and users.

Audits may include security scans to test for security vulnerabilities, and will be performed using automated tools of SITA's choice. Provider must correct any discovered vulnerabilities to the satisfaction of SITA within the time-period agreed with SITA.

SITA retains the right to investigate security incidents experienced by the Provider.