Third Party Information Security

CN Information Security - Guideline

Purpose

This Guideline articulates the high-level information security requirements that a Third Party should respect to protect CN's Information and IT Assets. All CN's Third Parties shall safeguard the availability, integrity and confidentiality of CN's Confidential Information. Furthermore, some Third Parties may be provided access to CN's IT Assets and as a consequence shall respect CN's corporate policies and standards to prevent cyber attacks on CN's IT Assets. Failure to do so could cause irreparable harm to CN's business, operations, reputation and financial standing.

Scope

This Guideline applies to all Third Parties who provide CN with Information Technology services, Operational Technology services or services whereby they host, store or access CN's Confidential Information. Additionally, when accessing CN's IT Assets, Third Parties shall comply with CN's corporate information security policies and security controls. CN will update its Third Party Information Security Guideline from time to time to reflect evolving technology, threats and security standards and Third Parties are encouraged to verify the Guideline from time to time. CN reserves the right to monitor its Third Parties' performance and compliance to the security standards included in CN's contractual documents.

Document details

Key dates

Published on 9/3/2018

Ownership: InfoSec

Table of Contents

Definitions

Confidential Information means protected information such as critical infrastructure information, sensitive security information and any information that is confidential by its nature, whether it is marked confidential or restricted or not, that is communicated by CN to a Third Party and that CN desires for a Third Party to keep confidential and use only for the purpose of its relationship with CN. Examples of Confidential Information include:

- CN's commercially or competitively sensitive, proprietary or private information including information of a business, commercial, industrial, scientific, strategic, or technical nature
- formulas, processes and mechanisms
- data, plans, drawings, in particular operational, commercial financial or investment plans
- business and strategic operating plans
- contracts and agreements
- corporate transactions, mergers and acquisitions
- internal communications, memoranda, presentations
- supplier lists
- CN's personal identifying information
- all data that is classified as CN-INTERNAL, CN-CONFIDENTIAL and CN-RESTRICTED, in any form including paper, electronic, video or voice recording data.
- CN Intellectual Property
- new product, brand and marketing strategies, plans and forecasts, strategic alliances, development of new products and business areas
- customer lists and contact information, needs, purchasing history, rates, specifications and preferences
- legal information including that covered by legal privilege
- competitive intelligence and market information compiled for CN
- information about CN's IT systems, infrastructure and operations
- corporate data
- CN's personal health information

Third Party means suppliers, governments, non-governmental organizations or any other entities (including their Personnel) with whom CN has a relationship and may share its Confidential Information with.

Personnel means Third Party's employees, agents, consultants, subcontractors or representatives, if any, involved in the supply of services.

CN IT Assets means the information technologies, operational technologies and environments, networks, equipment, computers, systems, devices, servers, applications, software, services, facilities and infrastructure.

1. Information Security Certifications, Frameworks and Standards

1.1. Third Parties shall implement a comprehensive and structured approach to protecting CN's Confidential Information. Their approach should include an information security program comprised of security policies, standards, procedures and controls. Third Party information security programs should either be aligned with, certified by, or adopt the current versions of, one or more of the following:

- ISO/IEC 27000 series information security standards and/or certifications
- NIST Cybersecurity Framework
- US Government FedRAMP certification
- Cloud Security Alliance (CSA) STAR certification
- AICPA SSAE 16 SOC 1 Type 2
- AICPA SOC 2 Type 2 Attestation or SSAE 18
- ISAE 3402 Assurance Standard applied to information security
- CSAE 3416 (Canadian equivalent to AICPA SOC 2)

1.2. Third Parties should evaluate and monitor their exposure to security risks and other threats and take appropriate measures to address the associated risks to their facilities, IT Assets, as well as CN Confidential Information.

1.3. Third Parties should review the following document titled AAR Rail Information Security Committee Cyber Security Effective Practices for Information Technology Procurement. This document is available at https://www.aar.org/data/cyber-security-effective-practices-for-information-technology-procurements/. It contains a set of recommended practices for securing rail systems.

1.4. Third Parties should formalize and document their information security program and security controls in a set of policies, standards, and procedures that can be made available to CN upon request.

2. Risk Management Programs and Methodologies

2.1. Third Parties should adopt a comprehensive and structured approach to risk management that identifies and mitigates risks associated with their IT Assets and information security program such as:

- ISO/IEC 27005
- ISACA COBIT 5
- NIST SP 800-30
- Information Security Forum IRAM 2
- FAIR

2.2. Third Parties should evaluate and monitor their exposure to information security risks and threats through regular review and take appropriate actions to address the associated risks to their IT Assets and CN's Confidential Information. Findings from these reviews shall be made available to CN upon request.

3. Security Controls

3.1. Third Parties should implement information security controls. A minimum set of examples would include:

- robust and documented change control processes, including regular release management cycles, preferably following well-known practices such as ITIL
- vulnerability management, security patches/fixes and changes to IT Assets shall be controlled and follow standard change management procedures and approved operational change windows, which, where appropriate, may be agreed between CN and Third Party
- development, test, production and/or backup environments that are physically and logically separated to reduce the risk of unauthorized access or changes to production environments
- controls to prevent changing, copying or altering any code belonging to CN without prior written permission
- back-up and retention policies that define frequency of back-ups and retention cycles for all data and environments as required for the performance of their services in accordance with any agreements for such services
- intrusion detection, prevention, and recovery controls that protect against malicious code and maintain all anti-virus software and signatures current and actively running to detect and remove malware
- detection tools that help protect users from downloading programs or other material from the Internet or use of any type of removable media (including USB, CD/DVD media) on Third Party IT Assets that may store, access or process CN Confidential Information unless they have been authenticated as originating from a trusted source and scanned for viruses
- password complexity standards to mitigate weak password threats
- network and physical perimeter security
- secure software development practices (commonly known as S-SDLC)

4. Security and Operational Log Management and Access

4.1. Third Party IT Assets should be configured with log management capabilities that:

- track security and operational events, incidents, activities, access to information or programs, system events such as alerts, console messages and system errors,

  and detection, prevention, and recovery controls with respect to all aspects of the relationship with CN and services managed by Third Party
- manage log lifecycles and retain them beyond the business services or relationship purpose, or longer where specified in the relevant agreement and/or where required by laws or regulations applicable to the services or relationship of the Third Party
- are protected against tampering and unauthorized access.

4.2. Third Parties may be asked to make relevant log information available to CN either regularly or upon request for audit and archival purposes.

5. Audit Rights

5.1. To perform security assessments, and upon reasonable notice, Third Parties shall permit CN or its partners (including government regulators requiring inspections of CN) to access CN's Confidential Information that is hosted, stored, accessed or otherwise processed in Third Party's IT Assets. Security assessments shall include, as applicable, the following:

- network vulnerability assessments
- review of high-level design and topology of the information security services
- review of configuration files for IT Assets
- review of technical and security controls in the data center and associated IT operations
- forensic investigations for cybersecurity incidents.

6. Compliance with CN Policies

6.1. When a Third Party accesses CN's IT Assets, CN's corporate information security policies, standards and procedures apply and the Third Party shall respect them and any specific instructions provided by CN with respect to a specific engagement, mandate, agreement, access or statement of work. In particular, it is forbidden for Third Parties to:

- attempt to circumvent or override CN's security controls
- act in a way that constitutes a violation of criminal law
- participating in phishing or other unauthorized access or disclosure schemes
- seek or gain unauthorized access to, or attack the integrity of, CN IT Assets or attempt to do so
- wilfully or recklessly spread computer viruses
- remove or tamper with security safeguards, controls or systems installed or configured by CN

- destroy, alter or encrypt CN Confidential Information, inadvertently or with the intent of making it inaccessible to CN
- intercept, listen in on or interfere with CN's voice, data or other electronic communications
- use CN IT Assets for any purpose other than the purpose they are intended for or the Third Party's defined mandate or services, notably it is prohibited to run a personal business or conduct business transactions unrelated to the performance of their duties for CN.

6.2. CN IT Assets that are made available to Third Parties remain CN's sole property. Third parties shall have no expectation of privacy when using CN's IT assets nor expect that anything that is stored or received on or sent from CN's IT Assets is Third Party's private property or information. In particular, CN may, from time to time monitor, review, intercept, access, modify or delete any files or communications stored on or exchanged through CN's IT assets, including non-business information, without notice.

7. Personnel

7.1. The Third Party is responsible for the acts and omissions of its Personnel and as such shall for all Personnel who may have access to Third Party IT Assets or have access to or custody of CN IT assets, facilities, and/or CN Confidential Information shall:

- conduct relevant background and reference checks
- provide suitable information security training and awareness program
- manage their Personnel's performance in securing CN's IT Assets and CN's Confidential Information.

8. Information Exchange Policies and Procedures

8.1. Third Parties shall use best practices for the exchange of information, for example, use secure managed file transfer services and/or secure email tools when sharing or exchanging CN Confidential Information with CN or any other Third Party.

9. Consequences of Non-Compliance to CN's Information Security Policies

9.1. Any Third Party who violates CN's information security policies may be subject to termination of the relationship or contract between the CN and Third Party.

9.2. CN may, at its sole discretion, remove a Third Party's access to CN's Confidential Information and/or certain IT Assets.

9.3. If Third Party’s behaviour is not compliant with applicable laws, this could also result in law enforcement, criminal prosecution or other legal action.