COLUMBUS REGIONAL AIRPORT AUTHORITY

Innovation & Technology | Cyber Security
Supplier Information Security Requirements

Last Modified

12/21/2023

Responsibility	Printed Name	Signature	Date
Approver	William Kellam		
Approver	Clifford O. Goshia		

Supplier Information Security Requirements

Contents

Supplier Information Security Requirements

1 Columbus Regional Airport Authority ("CRAA") Supplier Information SecurityRequirements (SISR)

Introduction: This CRAA Supplier Information Security Requirements ("Security Requirements") document provides guidance and direction to CRAA Suppliers and business partners for protecting CRAA information and assets.

Purpose: This document defines the minimum-security requirements that Suppliers and business partners must use to support the CRAA Information Security Program. The requirements detailed in this publication are intended to protect CRAA information assets.

Scope: These requirements apply to data in all forms, whether electronic, printed or written, for all products and services that use or support CRAA information, systems, network and/or applications in development, test, or production environments. In addition, these requirements are applicable to all Suppliers, business partners and other persons and/or organizations that perform business functions for the operating units of CRAA.

The following Security Requirements apply to the Supplier, its subcontractors, and each of their employees and/or temporary workers, contractors, suppliers, or agents who perform services for, or on behalf of, CRAA and include:

a) The collection, storage, handling, or disposal of CRAA information;
b) Connectivity to CRAA non-public networks and Information resources;
c) Custom software development or software implementation;

During the term of this agreement Supplier shall comply with the requirements set forth herein.

CRAA reserves the right to update or modify its Security Requirements from time-to-time. Upon written notification by CRAA of its intent to modify the Security Requirements, the Supplier agrees to promptly negotiate in good faith and expedite execution of an amendment to this agreement to incorporate any such modification. Supplier acknowledges that CRAA may require modifications to Security Requirements upon:

a) Extension, or renewal of the Agreement;
b) Any change in work scope or other substantive modification of the Agreement; or
c) Such time that CRAA deems appropriate or necessary.

Duration: The term of this agreement shall remain in effect for a 3-year period. Supplier must then renew their attestation to the Security Requirements, and notify CRAA of any changes in infrastructure that may affect their ability to comply; making note of any additions, updates, or modifications to each requirement.

Supplier Information Security Requirements

1.1 In accordance with Security Requirements, the Supplier shall:

1.1.1.1 Actively monitor industry resources (e.g., www.cert.org pertinent software Supplier mailing lists and websites) for timely notification of applicable security alerts.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.1.1.2 Scan externally facing Information Resources with applicable industry standard security vulnerability scanning software (including, but not limited to, network, server, and application scanning tools) monthly, at a minimum.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.1.1.3 Scan internal Information Resources with applicable industry standard security vulnerability scanning software (including, but not limited to, network, server,application, and database scanning tools) at a minimum monthly.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.1.1.4 Upon CRAA's request, provide current scanning results for the Information Resources.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.1.1.5 *Have, and use, a documented process to remediate security vulnerabilities including, but not limited to, those discovered through industry publications, vulnerability scanning, virus scanning, and the review of security logs, and apply appropriate security patches promptly with respect to the probability that such vulnerability can be or is in the process of being exploited.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.1.1.6 *Assign security administration responsibilities for configuring host operating systems to specific individuals.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.1.1.7 *Ensure that security staff has reasonable and necessary experience in information/network security.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.1.1.8 *Ensure that all the Supplier's Information Resources are, and remain, 'hardened' including, but not limited to, removing, or disabling unused network services (e.g., finger, rlogin, ftp, simple TCP/IP services) and installing a system firewall, TCP Wrappers or similar technology*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.1.1.9 Change all default account names and/or default passwords in accordance with the password requirements set forth herein.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.1.1.10 Limit system administrator/root (or privileged, super user, or the like) access to host operating systems only to individuals requiring such privileged access in the performance of their jobs.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.1.1.11 Require system administrators to restrict access by users to only the commands, data and Information Resources necessary to perform authorized functions.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.2 Physical Security

1.2.1.1 Ensure that all of Supplier's networks and Information Resources are in secure physical facilities with access limited and restricted to authorized individuals only.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.2.1.2 Monitor and record, for audit purposes, access to the physical facilities containing networks and Information Resources used in connection with Supplier's performance of its obligations under the Agreement.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

1.3 Network Security

1.3.1.1 When providing Internet-based services to CRAA, protect CRAA's Information by the implementation of a network demilitarized zone ("DMZ"). Web servers providing service to CRAA shall reside in the DMZ. Information Resources storing CRAA Information (such as application and database servers) shall reside in a trusted internal network.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.3.1.2 Upon CRAA's request, provide a logical network diagram detailing the Information Resources (including, but not limited to, firewalls, servers, etc.) that will support CRAA.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.3.1.3 Have a documented process, and controls in place to detect and handle unauthorized attempts to access CRAA Information.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.3.1.4 Use Strong Encryption for the transfer of CRAA Information outside of CRAA or Suppliercontrolled facilities, or when transmitting CRAA Information over any un-trusted network.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

1.4 Information Security

1.4.1.1 *Logically isolate CRAA's applications and Information from any other customer's or Supplier's own applications and information either by using physically separate servers or alternatively by using logical access controls (firewall) where physical separation of servers is not implemented.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.4.1.2 *Have a documented procedure for the secure backup, transport, storage, and disposal of CRAA Information and upon request, provide such documented procedure to CRAA.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.4.1.3 *Where physical and logical security of CRAA information cannot be assured, store CRAA information using a minimum of AES 256-bit encryption.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.4.1.4 *Limit access to CRAA Information to authorized persons or systems.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.4.1.5 *Be compliant with any applicable government-and industry-mandated information security standards as required by the type of CRAA information stored or transmitted by the Supplier. (Examples of such standards include, but are not limited to, the Payment Card Industry- Data Security Standards (PCI-DSS), Personal Identifiable Information (PII)*

Red Flag Rules (FTC) standards, and the information security requirements documented within laws, such as HIPAA.)

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.4.1.6 Unless otherwise instructed by CRAA, when collecting, generating, or creating Information for, through or on behalf of CRAA or under the CRAA brand, shall whenever practicable, label such Information as "Columbus Regional Airport Authority Proprietary Information" or at a minimum, label CRAA Information as "Confidential" or "Proprietary". Supplier acknowledges that CRAA Information shall remain CRAA-owned Information irrespective of labeling or absence thereof.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.5 Identification and Authentication

1.5.1.1 Assign unique User IDs and names to individual user's authentication credentials.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.5.1.2 Have and use a documented User Provisioning Lifecycle Management process including, but not limited to, procedures for approved account creation, timely account removal, and account modification (e.g., changes to privileges, span of access, functions/roles) for all Information Resources and across all environments (e.g., production, test, development, etc.).

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

1.5.1.3 Enforce the rule of least privilege (i.e., limiting access to only the commands and Information necessary to perform authorized functions according to one's job function).

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.5.1.4 Limit failed login attempts to no more than Five (5) successive attempts and lock the user account upon reaching limit. Access to the user account can be reactivated subsequently through a manual process requiring verification of the user's identity or, where such capability exists, can be automatically reactivated after at least three (3) minutes from the last failed login attempt.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.5.1.5 Require password expiration at regular intervals not to exceed ninety (90) days, .unless authorized in writing by CRAA.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.5.1.6 Use an authentication method based on the sensitivity of Information. When passwords are used, they must meet these minimum requirements:

a) Minimum of twelve (12) characters in length
b) *Contain all of the following complexity requirements: alpha, numeric, and special characters.*

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.5.1.7 Use a secure method for the conveyance of authentication credentials (e.g. passwords) and authentication mechanisms (e.g. tokens or smart cards).

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.5.1.8 Require implementation of multi-factor authentication and SSO for SAML v2.0 apps with all accounts created for use by CRAA employees and Supplier/service accounts created to access CRAA assets. This includes remote access to any Information Resources.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.6 Software and Data Integrity

1.6.1.1 Have current antivirus software installed and running to scan for and promptly remove viruses.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.6.1.2 Separate non-production Information Resources from production Information Resources.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

1.6.1.3 For applications which utilize a database that allows modifications to CRAA Information, have database transaction logging features enabled and retain database transaction logs for a minimum of ninety (90) days.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.6.1.4 For all software developed, used, furnished and/or supported under this Agreement, review such software to find and remediate security vulnerabilities during initial implementation and upon any modifications and updates.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.6.1.5 Perform quality assurance testing for the application functionality and security components (e.g., testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture) during initial implementation and upon any modifications and updates.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

1.7 Privacy Issues

1.7.1.1 Do not store CRAA information on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, external hard drives) except: (a) for backup and data interchange purposes as allowed and required under contract, and (b) using Strong Encryption.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.8 Monitoring and Auditing Controls

1.8.1.1 Restrict access to security logs to authorized individuals.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.8.1.2 Review security logs for anomalies, on no less than a weekly basis. Document and resolve all logged security problems in a timely manner.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

Supplier Information Security Requirements

1.8.1.3 Permit CRAA to conduct an audit to verify Supplier's compliance with CRAA SupplierInformation Security Requirements. Upon CRAA's written request for audit, the Supplier shall schedule a security audit to commence within a reasonable period and during normal business hours, but in no event more than thirty (30) days fromsuch request. In the event CRAA, in its sole discretion, deems that a security breach has occurred, the Supplier shall schedule the audit to commence within one (1) day of CRAA's notice requiring an audit. This provision shall not bedeemed to and shall not limit any more stringent audit obligations permitting theexamination of the Supplier's records contained in this Agreement. After completion of the audit, CRAA will provide a written audit report detailing the result of the audit.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.8.1.4 Within thirty (30) days of receipt of the audit report, Supplier will provide CRAA a written report outlining the corrective actions that Supplier has implemented or proposes to implement with the schedule and status of each corrective action. Supplier shall update this report to CRAA every thirty (30) days reporting the status of all corrective actions through the date of implementation. Supplier shall implement all corrective actions within ninety (90) days of Supplier's receipt of the audit report.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

1.9 Reporting Violations

1.9.1.1 ***Follow an established documented procedure*** in the event of an actual or suspected unauthorized intrusion or other security violation, including but not limited to, a physical security or computer security incident (*e.g.*, hacker activity or the introduction of a virus or malicious code), that involves any Information Resources used in conjunction with supporting CRAA and/or used by Supplier in fulfillment of its obligations under this Agreement, which includes immediate notification to the CRAA Help Desk or IT Security staff. ***Phone: 1 614.239.3050 (Service Desk number)***

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.9.1.2 ***Provide CRAA with regular status updates on any actual or suspected unauthorized intrusion or other security violation, that involves any Information Resources used in conjunction with supporting CRAA by the Supplier in fulfillment of its obligations under this agreement, including, but not limited to, actions taken to resolve such incident, at four (4) hour intervals (or at other mutually agreed intervals or times) for the duration of the incident, and within five (5) days of the closure of the incident, a written report describing the incident, actions taken by the Supplier during its response and Supplier's plans for future actions to prevent a similar incident from occurring.***

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.9.1.3 ***Upon notification by CRAA personnel of a vulnerability present in Supplier environment, tooling, hardware, software, or systems supporting CRAA assets, Supplier will remediate according to the information provided within ninety (90) days of notification or provide a compensating control that can be put into place, as agreed to by CRAA.***

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

1.10 Security Policies and Procedures

1.10.1.1 Ensure that all personnel, subcontractors, or representatives performing work on any CRAA Information Resources or the resources used to interconnect to CRAA resources, or the resources used to house CRAA Information under this Agreement are in compliance with CRAA Security Requirements.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.10.1.2 At a minimum, annually review CRAA Security Requirements to ensure that Supplier is in compliance with the requirements.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.11 Cyber Liability Insurance

1.11.1.1 Obtain and maintain an adequate level (See 1.11.1.3) of Third-Party Cyber Liability Insurance to manage risks associated with Supplier's Product(s) that use or support CRAA information assets, systems, network, and/or applications in development, test, or production.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:CRAA Response:

1.11.1.2 Provide CRAA with evidence of Cyber Liability Insurance coverage within thirty (30) days of request.

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance

Explanation:

CRAA Response:

1.11.1.3 Suppliers should maintain levels of coverage relating to their line of work referenced in the chartbelow.

Third Party Cyber Liability Insurance Requirements

Level of Coverage	Criteria
1 Million dollars	All Vendors subject to a VISR will be subject to this criteria at a minimum.
2 Million dollars	Any Vendor responsible for CRAA' data in any capacity.
3 Million dollars	Any Vendor that supports any CRAA system deemed business critical.
4 Million dollars	Any Vendor that will be hosting their equipment in CRAA' infrastructure wether that be hardware or software.
5 Million dollars	Any Vendor dealing directly with any PCI, PII, LEADS, HIPAA , or any other sensitive information relating to CRAA assets that also has a footprint in CRAAs internal or external facing network.

Supplier Information Security Requirements

Supplier will comply ☐ Yes ☐ No

Supplier Non-Compliance Explanation:

CRAA Response:

By signing below, Supplier represents that the responses and information it has provided herein are true and accurate as of the date indicated below. In addition, Supplier acknowledges its' affirmative and continuing duty to inform CRAA if any of Supplier's responses and information change during the course of its engagement with CRAA.

Supplier	
Email	
Name	
Telephone	
Title	
Date	
Signature	

CRAA Office	Contact	Telephone	E-mail
Cyber Security & Networking Cyber Security	Clifford Goshia William Kellam	(614) 239-3119 (614) 239-5067	cgoshia@columbusairports.com wdkellam@columbusairports.com