



ALLEGHENY COUNTY AIRPORT AUTHORITY

**PITTSBURGH INTERNATIONAL AIRPORT
ALLEGHENY COUNTY AIRPORT**

Cybersecurity and Privacy Vendor Review Policy

Document Version: 1.0.0

08 September 2022

Prepared by:

Theresa G. Blackwell-Frank, M.Ps., CISM, CISSP
Chief Information Security Officer (CISO)

Janice K. Kook, CISSP
Information Security Officer (ISO)

Reviewed by:

Title 1	
Title 2	
Title 3	
Title 4	
Title 5	
Title 6	

Change Record

Date	Version	Author	Changes Made / Section(s)
08 September 2022	1.0.0	Theresa G. Blackwell-Frank	Initial Document
10 February 2023	1.1	Janice Kook	Appendix L Added

Amplifying Guidance

- i. [National Institute of Standards and Technology \(NIST\) Recommended *Minimum Standard for Vendor or Developer Verification of Code*](#)
- ii. [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-88, *Guidelines for Media Sanitization*](#)
- iii. [ISO/IEC 27001 Information Security Management](#)

Table of Contents

1.0	Introduction	4
2.0	Right to Audit	4
3.0	Security Management	4
4.0	Risk Management	4
5.0	Personnel Security/Human Resources Security	4
6.0	Operations Management	5
7.0	Security Breach	5
8.0	Encryption and Data Management Controls	6
9.0	Access Controls	7
10.0	Vulnerability and Patch Management	7
11.0	Business Continuity and Disaster Recovery	8
12.0	Compliance	8
	APPENDIX A – RIGHT TO AUDIT VENDOR RESPONSE	9
	APPENDIX B – SECURITY MANAGEMENT VENDOR RESPONSE	10
	APPENDIX C – RISK MANAGEMENT VENDOR RESPONSE	11
	APPENDIX D – PERSONNEL SECURITY + HUMAN RESOURCES SECURITY VENDOR RESPONSE	12
	APPENDIX E – OPERATIONS MANAGEMENT VENDOR RESPONSE	13
	APPENDIX F – SECURITY BREACH VENDOR RESPONSE	14
	APPENDIX G – ENCRYPTION AND DATA MANAGEMENT CONTROLS VENDOR RESPONSE	16
	APPENDIX H – ACCESS CONTROLS VENDOR RESPONSE	17
	APPENDIX I – VULNERABILITY AND PATCH MANAGEMENT VENDOR RESPONSE	19
	APPENDIX J – BUSINESS CONTINUITY AND DISASTER RECOVERY VENDOR RESPONSE	20
	APPENDIX K – COMPLIANCE VENDOR RESPONSE	21
	APPENDIX L – CONSTRUCTION VENDOR RESPONSE	22

1.0 Introduction

Any vendor or supplier ("Vendor") supporting Allegheny County Airport Authority ("ACAA") is expected to implement and maintain the minimum information security requirements, as set forth below (and as applicable to the scope of services provided to ACAA).

2.0 Right to Audit

Vendor shall maintain all necessary documentation to show compliance with the minimum information security requirements set forth herein. Upon request, vendors shall permit ACAA or an independent third-party to audit Vendor's compliance with minimum information security requirements. To the extent required and applicable to the scope of work, Vendor must provide ACAA with written audit results as follows:

- Audit results shall be an ISO/ICE 27000 or other appropriate industry standard certification or report. The Vendor's information security management program shall comply with internationally recognized standard (i.e. ISO/IEC, NIST).
- If any such audit reveals material gaps or weaknesses in Vendor's security program, ACAA shall be entitled to suspend transmission of ACAA information to Vendor. Vendor is to cease processing of any information until such issues are resolved to the satisfaction of ACAA.
- ACAA reserves the right to terminate Vendor services without penalty if identified gaps or weaknesses are not resolved within a reasonable period.
- Vendor shall retain audit results for a minimum of thirty (30) days.

3.0 Security Management

Vendor shall maintain a comprehensive written information security program, based on best practice standards for their industry. The program, at minimum, must contain the following:

- Written information privacy and security policies, communicated to appropriate personnel and third-party providers and revised on a regular basis.
- Security training and awareness activities performed regularly and designed to enable employees and contractors to identify information privacy risks.

4.0 Risk Management

Vendor shall implement a risk management program to formally identify, assess, mitigate, and monitor risks regarding the Vendor's business and in compliance with internationally recognized standard (i.e. NIST). Vendor shall perform periodic risk assessments to evaluate the risk profile regarding the collection, transmission, storage, and usage of ACAA information. Vendor shall use best efforts to continuously monitor for the identification and mitigation efforts to internal and external risks that could result in the negative impact to ACAA information, information systems, operations, personnel, and/or property.

5.0 Personnel Security/Human Resources Security

Vendor shall implement controls to enable employees, contractors, and service providers to adhere to policies and standards, according to roles and access in order to reduce the risk of theft, fraud, loss, and misuse of facilities and/or information. At minimum, the Vendor shall:

- Ensure that employees, contractors, and third-party users understand their responsibilities and are suitable for the roles in which they are considered, including through any appropriate personnel screening.
- Security roles and responsibilities of employees, contractors, and third-party users must be defined and documented to incorporate ACAA data protection control requirements, including background checks to the extent permitted by applicable law.
- All employees, contractors, and third-party users must be provided with education and training in privacy and security procedures and the correct information processing requirements.
- If Vendor has knowledge that anyone is using or disclosing ACAA information in a manner outside of the scope of services, Vendor shall take reasonable steps to prevent or stop the use or disclosure
- Vendor is fully responsible in ensuring that only those with authorized access has access to ACAA information.

6.0 Operations Management

Vendor shall provide appropriate security and protection from unauthorized access, damages and interference of assets based on classification and/or information sensitivity. Vendor shall meet the minimum requirements as follows:

- All assets used to manage or store ACAA information must be protected against unauthorized access, disclosure, modification, destruction, or interference.
- All software used by Vendor in providing services to ACAA must be properly licensed before entering into an agreement/contract with ACAA.
- Vendors shall ensure that media sanitization of assets conforms to an industry accepted Media Sanitization standard (i.e. NIST SP 800-88).

Vendor is responsible for flowing down all requirements to subcontractors, to include but not limited to, data protection, privacy compliance, and security control validation/certification of sub-contractor information system(s).

7.0 Security Breach

Vendor shall comply with specified incident response processes for ACAA information and information systems. Vendor shall follow documented responsibilities and procedures to respond to information security incidents quickly, effectively, and in an orderly way. "Security Breach" means any act or omission that compromises either the security, confidentiality, integrity, and/or availability of ACAA information, or the physical, technical, administrative, or organizational safeguards put in place that relate to the overall security, confidentiality, integrity, and/or availability of ACAA information.

In the event it is determined that the Vendor is responsible for the security breach, the Vendor shall bear all costs associated with resolving a security breach, including those costs associated with conducting an investigation, notifying consumers and others as required by law or the relevant Security Standard (i.e. PCI-DISS). Vendor shall report any Security Breach through appropriate management channels as quickly as possible. Any Security Breach involving or impacting ACAA or an ACAA affiliate or subsidiary shall be reported to ACAA. Notification shall be within twenty-four (24) hours from detection of compromise to any ACAA information or asset.

Vendors shall cooperate with ACAA in investigations of any incidents involving ACAA information and/or information systems. Vendor shall cooperate with ACAA personnel, affiliates, and representatives in responding to inquiries, claims, and complaints regarding the processing of ACAA information, including but not limited to:

- Assisting with any investigation as requested by ACAA.
- Providing ACAA with physical access to facilities and affected operations.
- Facilitating interviews with Vendor's representatives and others involved in the matter.
- Making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards, or as otherwise reasonably requested by ACAA.

Vendor is responsible for informing third-party(ies) of any security breach, which affects ACAA, without first obtaining the prior written consent of ACAA, other than to inform a complainant that the matter has been forwarded to ACAA legal counsel. ACAA shall have the sole right and authority to determine the following:

- Whether notice of the security breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in ACAA's discretion.
- The contents of such notice.
- Whether any remediation may be offered to affected persons.
- The nature and extent of any such remediation.

8.0 Encryption and Data Management Controls

Cryptographic controls shall be used to protect the confidentiality, integrity, and availability of ACAA information in transit and while in Vendor's possession, to include data at rest. Controls for the management and use of cryptographic keys must be developed, implemented, and reviewed by Vendor on a periodic basis. Vendors shall encrypt the following:

- Desktops, laptops, and all other portable devices storing ACAA information.
- All messages and files containing ACAA information during transit over public networks.

If the processing involves the transmission of ACAA information over a network, Vendor shall have implemented appropriate supplementary measures to protect ACAA information against the specific risks presented by network processing. ACAA information shall only be transmitted in an encrypted format. ACAA information may not be stored on any portable computer devices or media (including laptop, computer, other portable devices, and all forms of removable media) unless the ACAA information is encrypted, or the removable media containing ACAA information is fully encrypted. Vendor shall be aware of any regulations, standards, or industry or sector specific guidelines that set forth minimum guidelines for encrypting personal data.

9.0 Access Controls

At minimum, Vendor shall meet the following access control requirements:

- Access to resources, including ACAA information, shall be regulated by using information security access controls and authorization mechanisms aligned with risk.
- Vendor shall secure its computer networks using multiple layers of access controls to protect against unauthorized access.
- Vendor shall secure remote access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or tightly controlling access through management approvals, robust controls, logging and monitoring access events and subsequent audits.
- Vendor shall deploy multi-factor authentication or single sign-on measures where possible to its systems containing ACAA information or any external system with potential access to ACAA information.
- Vendor shall limit access to the minimum necessary to perform required function.
- Vendor shall maintain and enforce a password policy which addresses password length, composition, complexity, lockout, history, and expiration.
- Vendor shall revoke access for any Vendor employee, contractor, or third-party user of ACAA information, and facilities processing ACAA information, upon their termination of employment contract or agreement, or adjusted access upon a change of responsibility, within 24 hours.
- Vendor shall define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of physical penetration by malicious or unauthorized personnel, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.
- Vendor shall appropriately leverage firewall infrastructure to segregate sensitive environments and restrict the use of insecure protocols. Network segments connected to the internet must be protected by a firewall, which is configured to secure all devices behind it.

10.0 Vulnerability and Patch Management

Vendor shall have appropriate vulnerability management controls to identify and mitigate deficiencies and weaknesses within their network(s), system(s), and software. At minimum, vendor shall meet the following:

- Vendor shall conduct periodic vulnerability scans to identify vulnerabilities.
- Vendor shall prioritize remediation of identified vulnerabilities aligned to risk level and remediation schedule.
- Vendor shall conduct period penetration testing and/or comparable vulnerability assessment aligned to current industry standards; upon request, Vendor shall provide a copy of the report from latest penetration testing or vulnerability assessment results to include remediation progress.
- Vendor shall have a formal patch management schedule and controls to identify, test, and implement all required industry patches; industry patches shall be applied immediately upon availability.

11.0 Business Continuity and Disaster Recovery

Vendor shall have appropriate Business Continuity and Disaster Recovery plans that meet the following minimum requirements:

- Prevent or mitigate business interruption and associated impact relating to serviced parties.
- Address ongoing access to ACAA information to satisfy contractual servicing agreement(s).
- Business Continuity and Disaster Recovery capability shall be tested regularly.

12.0 Compliance

Vendor information security and data protection controls and processes shall comply with applicable law and contractual obligations. If Vendor is unable to comply, ACAA shall be notified immediately.

PCI Data Security Standards. If Vendor has access to or will create, receive, store, process, or transmit ACAA cardholder information (i.e. credit, debit, stored value, prepaid card information), Vendor, at its own expense, shall meet the following minimum requirements:

- Vendor shall assume full responsibility for security cardholder information in its care, custody, possession, or control.
- Vendor shall comply with the applicable current Payment Card Industry Data Security Standards (PCI Standards).
- Vendor shall provide ACAA with an annual third-party Attestation of Compliance.

HIPAA Protected Health Information. If Vendor has access to or will create, receive, store, process, or transmit Protected Health Information, Vendor, at its own expense, shall meet the following minimum requirements:

- Vendor shall assume full responsibility for security Personal Health Information in its care, custody, possession, or control.
- Vendor shall comply with HIPAA, including all applicable privacy and security standards.

APPENDIX A – RIGHT TO AUDIT | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall maintain all necessary documentation to show compliance with the minimum information security requirements set forth herein. Upon request, vendors shall permit ACAAA or an independent third-party to audit Vendor's compliance with minimum information security requirements.	
Vendor must provide ACAAA with written audit results as follows: • Audit results shall be an ISO/ICE 27000 or other appropriate industry standard certification or report. The Vendor's information security management program shall comply with internationally recognized standard (i.e. ISO/IEC, NIST). • If any such audit reveals material gaps or weaknesses in Vendor's security program, ACAAA shall be entitled to suspend transmission of ACAAA information to Vendor. Vendor is to cease processing of any information until such issues are resolved to the satisfaction of ACAAA. • ACAAA reserves the right to terminate Vendor services without penalty if identified gaps or weaknesses are not resolved within a reasonable period. • Vendor shall retain audit results for a minimum of thirty (30) days.	

APPENDIX B – SECURITY MANAGEMENT | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall maintain a comprehensive written information security program, based on best practice standards for their industry.	
Information security program, at minimum, must contain the following: • Written information privacy and security policies, communicated to appropriate personnel and third-party providers and revised on a regular basis. • Security training and awareness activities performed regularly and designed to enable employees and contractors to identify information privacy risks.	

APPENDIX C – RISK MANAGEMENT | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall implement a risk management program to formally identify, assess, mitigate, and monitor risks regarding the Vendor's business and in compliance with internationally recognized standard (i.e. NIST).	
Vendor shall perform periodic risk assessments to evaluate the risk profile regarding the collection, transmission, storage, and usage of ACAA information.	
Vendor shall use best efforts to continuously monitor for the identification and mitigation efforts to internal and external risks that could result in the negative impact to ACAA information, information systems, operations, personnel, and/or property.	

APPENDIX D – PERSONNEL SECURITY + HUMAN RESOURCES SECURITY | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall implement controls to enable employees, contractors, and service providers to adhere to policies and standards, according to roles and access in order to reduce the risk of theft, fraud, loss, and misuse of facilities and/or information.	
Ensure that employees, contractors, and third-party users understand their responsibilities and are suitable for the roles in which they are considered, including through any appropriate personnel screening.	
Security roles and responsibilities of employees, contractors, and third-party users must be defined and documented to incorporate ACAA data protection control requirements, including background checks to the extent permitted by applicable law.	
All employees, contractors, and third-party users must be provided with education and training in privacy and security procedures and the correct information processing requirements.	
If Vendor has knowledge that anyone is using or disclosing ACAA information in a manner outside of the scope of services, Vendor shall take reasonable steps to prevent or stop the use or disclosure	
If Vendor has knowledge that anyone is using or disclosing ACAA information in a manner outside of the scope of services, Vendor shall take reasonable steps to prevent or stop the use or disclosure	
Vendor is fully responsible in ensuring that only those with authorized access has access to ACAA information.	

APPENDIX E – OPERATIONS MANAGEMENT | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall provide appropriate security and protection from unauthorized access, damages and interference of assets based on classification and/or information sensitivity.	
All assets used to manage or store ACAA information must be protected against unauthorized access, disclosure, modification, destruction, or interference.	
All software used by Vendor in providing services to ACAA must be properly licensed before entering into an agreement/contract with ACAA.	
Vendors shall ensure that media sanitization of assets conforms to an industry accepted Media Sanitization standard (i.e. NIST SP 800-88).	
Vendor is responsible for flowing down all requirements to subcontractors, to include but not limited to, data protection, privacy compliance, and security control validation/certification of sub-contractor information system(s).	

APPENDIX F – SECURITY BREACH | VENDOR RESPONSE

“Security Breach” means any act or omission that compromises either the security, confidentiality, integrity, and/or availability of ACAA information, or the physical, technical, administrative, or organizational safeguards put in place that relate to the overall security, confidentiality, integrity, and/or availability of ACAA information.

ACAA Requirement	Vendor Response
Vendor shall comply with specified incident response processes for ACAA information and information systems.	
Vendor shall follow documented responsibilities and procedures to respond to information security incidents quickly, effectively, and in an orderly way.	
Vendor shall bear all costs associated with resolving a security breach, including those costs associated with conducting an investigation, notifying consumers and others as required by law or the relevant Security Standard (i.e. PCI-DISS).	
Vendor shall report any Security Breach through appropriate management channels as quickly as possible.	
Any Security Breach involving or impacting ACAA or an ACAA affiliate or subsidiary shall be reported to ACAA. Notification shall be within twenty-four (24) hours from detection of compromise to any ACAA information or asset.	
Vendors shall cooperate with ACAA in investigations of any incidents involving ACAA information and/or information systems.	
Vendor shall cooperate with ACAA personnel, affiliates, and representatives in responding to inquiries, claims, and complaints regarding the processing of ACAA information, including but not limited to: • Assisting with any investigation as requested by ACAA. • Providing ACAA with physical access to facilities and affected operations. • Facilitating interviews with Vendor’s representatives and others involved in the matter. • Making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law,	

regulation, industry standards, or as otherwise reasonably requested by ACAA.	
Vendor is responsible for informing third-party(ies) of any security breach, which affects ACAA, without first obtaining the prior written consent of ACAA, other than to inform a complainant that the matter has been forwarded to ACAA legal counsel.	
ACAA shall have the sole right and authority to determine the following: • Whether notice of the security breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in ACAA's discretion. • The contents of such notice. • Whether any remediation may be offered to affected persons. • The nature and extent of any such remediation.	

APPENDIX G – ENCRYPTION AND DATA MANAGEMENT CONTROLS | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Cryptographic controls shall be used to protect the confidentiality, integrity, and availability of ACAA information in transit and while in Vendor's possession, to include data at rest.	
Controls for the management and use of cryptographic keys must be developed, implemented, and reviewed by Vendor on a periodic basis.	
Vendors shall encrypt the following: • Desktops, laptops, and all other portable devices storing ACAA information. • All messages and files containing ACAA information during transit over public networks.	
If the processing involves the transmission of ACAA information over a network, Vendor shall have implemented appropriate supplementary measures to protect ACAA information against the specific risks presented by network processing.	
ACAA information shall only be transmitted in an encrypted format.	
ACAA information may not be stored on any portable computer devices or media (including laptop, computer, other portable devices, and all forms of removable media) unless the ACAA information is encrypted, or the removable media containing ACAA information is fully encrypted.	
Vendor shall be aware of any regulations, standards, or industry or sector specific guidelines that set forth minimum guidelines for encrypting personal data.	

APPENDIX H – ACCESS CONTROLS | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Access to resources, including ACAA information, shall be regulated by using information security access controls and authorization mechanisms aligned with risk.	
Vendor shall secure its computer networks using multiple layers of access controls to protect against unauthorized access.	
Vendor shall secure remote access to and from its systems by disabling remote communications at the operating system level if no business need exists and/or tightly controlling access through management approvals, robust controls, logging and monitoring access events and subsequent audits.	
Vendor shall deploy multi-factor authentication or single sign-on measures where possible to its systems containing ACAA information or any external system with potential access to ACAA information.	
Vendor shall limit access to the minimum necessary to perform required function.	
Vendor shall maintain and enforce a password policy which addresses password length, composition, complexity, lockout, history, and expiration.	
Vendor shall with revoke access for any Vendor employee, contractor, or third-party user of ACAA information, and facilities processing ACAA information, upon their termination of employment contract or agreement, or adjusted access upon a change of responsibility, within 24 hours.	
Vendor shall define physical security zones and implement appropriate preventative and detective controls in each zone to protect against the risks of physical penetration by malicious or unauthorized personnel, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.	
Vendor shall appropriately leverage firewall infrastructure to segregate sensitive environments and restrict the use of insecure	

protocols. Network segments connected to the internet must be protected by a firewall, which is configured to secure all devices behind it.	
---	--

APPENDIX I – VULNERABILITY AND PATCH MANAGEMENT | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall have appropriate vulnerability management controls to identify and mitigate deficiencies and weaknesses within their network(s), system(s), and software.	
Vendor shall conduct periodic vulnerability scans to identify vulnerabilities.	
Vendor shall prioritize remediation of identified vulnerabilities aligned to risk level and remediation schedule.	
Vendor shall conduct period penetration testing and/or comparable vulnerability assessment aligned to current industry standards; upon request, Vendor shall provide a copy of the report from latest penetration testing or vulnerability assessment results to include remediation progress.	
Vendor shall have a formal patch management schedule and controls to identify, test, and implement all required industry patches; industry patches shall be applied immediately upon availability.	

APPENDIX J – BUSINESS CONTINUITY AND DISASTER RECOVERY | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall have appropriate Business Continuity and Disaster Recovery plans that meet the following minimum requirements: • Prevent or mitigate business interruption and associated impact relating to serviced parties. • Address ongoing access to ACAA information to satisfy contractual servicing agreement(s). • Business Continuity and Disaster Recovery capability shall be tested regularly.	

APPENDIX K – COMPLIANCE | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor information security and data protection controls and processes shall comply with applicable law and contractual obligations. If Vendor is unable to comply, ACAA shall be notified immediately.	
PCI Data Security Standards. If Vendor has access to or will create, receive, store, process, or transmit ACAA cardholder information (i.e. credit, debit, stored value, prepaid card information), Vendor, at its own expense, shall meet the following minimum requirements: • Vendor shall assume full responsibility for security cardholder information in its care, custody, possession, or control. • Vendor shall comply with the applicable current Payment Card Industry Data Security Standards (PCI Standards). • Vendor shall provide ACAA with an annual third-party Attestation of Compliance.	
HIPAA Protected Health Information. If Vendor has access to or will create, receive, store, process, or transmit Protect Health Information, Vendor, at its own expense, shall meet the following minimum requirements: • Vendor shall assume full responsibility for security Personal Health Information in its care, custody, possession, or control. • Vendor shall comply with HIPAA, including all applicable privacy and security standards.	

APPENDIX L – CONSTRUCTION | VENDOR RESPONSE

ACAA Requirement	Vendor Response
Vendor shall comply with safety standards for construction developed by the National Institute of Standards and Technology (NIST) - https://www.nist.gov/buildings-construction. If Vendor is unable to comply, ACAA shall be notified immediately. • Building codes and standards. • Building damage and repair. • Building materials. • Heating, ventilation and air conditioning equipment. • Structural Engineering. • Building control systems. • Building economics. • Energy efficiency. • Indoor air quality. • Thermal comfort.	
Where applicable, Vendor shall reference published studies from the National Institute of Standards and Technology (NIST) to incorporate into construction and hazard planning: • National Earthquake Hazards Reduction Program (NEHRP) • National Windstorm Impact Reduction Program (NWIRP)	
Vendor shall comply with <i>Title 6 Code of Federal Regulations (CFR) part 29, Procedures for Handling Critical Infrastructure Information; Final Rule</i> in efforts to safeguard the receipt, validation, handling, storage, marking, and use of critical infrastructure information (CII) to ensure that sensitive or proprietary data is not disclosed to the public and/or unauthorized parties.	