# ARABELLE SOLUTIONS THIRD PARTY CYBER SECURITY REQUIREMENTS

**Prepared by:** Arabelle Solutions 3rd Party Security Team

**Version:** 1.0

**Effective Date:** June 1, 2024

## 1. INTRODUCTION

The Arabelle Solutions (ARS) Third-Party Cyber Security Requirements document outlines the cyber security requirements applicable to ARS third parties, including suppliers and joint ventures. The security requirements outlined herein, are applicable to third parties that process, access, interact with, or store ARS sensitive Information (classified internally as ARS Confidential or ARS Highly Confidential), PII or Sensitive PII, have access to a ARS Information System, or provide certain services/products, to include OT/Manufacturing services, as described below. The security requirements are designed to vary based on the level of risk the Third-Party presents to ARS, specifically guided by the type of ARS information the Third-Party processes, network connection, and products and services provided by the Third-Party, as well as data availability and resiliency requirements. In addition to ARS cyber security requirements, third parties are required to abide by applicable regulatory requirements.

Cyber security requirements mentioned in this document are high level security requirements and actual cyber security controls will be discussed during ARS security assessment. ARS reserves the right periodically to update this document.

ARS reserves the right to update this document from time to time.

## 2. IT SECURITY REQUIREMENTS

**Applicability:** IT security requirements are applicable to third parties that process, access, or stores ARS Confidential Information, Personal Data, ARS Highly Confidential Information, Sensitive Personal Data, Controlled Data, or if the Third-Party has a direct network connection to the ARS managed network.

| IT SECURITY REQUIREMENTS | |
|---|---|
| 2.1 | Third-Party must have a documented and evidenced identity and access management process for granting, modifying, and revoking access to ensure confidentiality, integrity, and availability of systems used to access, process, store and transmit ARS Data |
| 2.2 | Third-Party must enforce strong password requirements on their IT assets. |
| 2.3 | Third-Party must change default passwords of all their IT assets. |
| 2.4 | Third-Party must centrally manage user accounts especially privileged accounts (using RSA, RADIUS, TACACS, LDAP etc.). |
| 2.5 | Third-Party must ensure that all administrators use two accounts; regular accounts for normal activities and domain administrator accounts for activities requires escalated privileges. |
| 2.6 | Third-Party must ensure that security relevant events logs are reviewed & stored for at least 90 days on all servers (Including but not Limited to DHCP & DNS servers) and critical network devices (e.g., firewalls, Intrusion Detection System, routers, etc.). |
| 2.7 | If a Third-Party experienced a ransomware attack, data breach, or other significant cyber event in the last 24 months then they must provide detailed information on the breach that was identified, impact, and how it was remediated.<br>Also, if a Third-Party identifies any cyber breach, they must inform raiseaconcern@arabellesolutions.com, & their Arabelle Solutions Business SPOC. |
| 2.8 | Third-Party must have a documented change control process in place. |
| 2.9 | Third-Party must have DLP controls in place which includes URL filtering to block access to high-risk sites and non-sanctioned file sharing sites/applications, host-based Data Loss Prevention (DLP), network based DLP, blocking of USB ports etc. |
| 2.10 | Third-Party must have a process to protect cryptographic keys if they are used to encrypt ARS data |
| 2.11 | Third-Party must ensure to store ARS data in encrypted form using an encryption algorithm equivalent to AES 118, 191, or 156. |
| 2.12 | Third-Party must have Endpoint Detection and Response (EDR) capabilities implemented on all applicable IT assets. |
| 2.13 | Third-Party must not utilize any high-risk technologies mentioned in US FCC's covered list in the IT environment being used by ARS. Refer https://www.fcc.gov/supplychain/coveredlist for details. |
| 2.14 | Third-Party must have a documented information security incident management plan that is tested at least annually |

| | |
|---|---|
| 2.15 | Third-Party must maintain an inventory of all their IT assets including physical devices, software, internally and externally hosted applications, cloud providers, third-party network connections etc. |
| 2.16 | Third-Party must have a comprehensive network security program in place. |
| 2.17 | Third-Party must have network level intrusion detection or prevention system to monitor their network 14x7x365 and a process to act on critical & high alerts. |
| 2.18 | Third-Party must have enforced secure wireless encryption protocol (e.g., WPA1) to connect to their organization's Wi-Fi. |
| 2.19 | Third-Party must enforce multi-factor authentication while connecting remotely to company network. |
| 2.20 | Third-Party must have a patch management process which includes applying all relevant vendor rated critical patches and security updates within 30 days of release by the vendor. |
| 2.21 | Third-Party must not use any end of life (EOL) technology. |
| 2.22 | Third-Party must perform periodic security awareness training and assessment. |
| 2.23 | If Third-Party need to outsource any ARS related work and have to share ARS data to their suppliers/contractors, they must have a process to identify, assess and manage supply chain cyber risks and perform cyber security assessments of their suppliers/contractors before sharing ARS data. |
| 2.24 | Third-Party must perform at least annual network vulnerability assessment or penetration test on the local & cloud IT infrastructure which store, process, host, or transmit ARS data |
| 2.25 | If Third-Party use application(s) to store, process, host, and/or transmit ARS data they must perform annual web application vulnerability assessment or penetration test. |
| 2.26 | Third-Party must have a policy to remediate all critical or high rated security vulnerabilities or issues within 30 days of identification. This includes issues identified in IT security audits or vulnerabilities identified in network or web application vulnerability assessments or penetration test |
| 2.27 | Third-Party must configure session timeouts on all IT assets. Recommended ideal session timeout for workstations and servers is 15 minutes and for applications it is 30 minutes. |
| 2.28 | Third-Party must have a controls/process in place to ensure only authorized software will be installed on desktops, laptops, and servers. |
| 2.29 | Third-Party must have a mechanism in place to make sure no one has access to tamper logs on their SIEM/local systems. |
| 2.30 | Third-Party must perform pre-employment background screening for those who require access to ARS data, systems, or work in ARS project |
| 2.31 | Third-Party must not store ARS data on any removable media. If there is any such requirement, it must be approved by ARS business counterpart and the backup media must be encrypted |
| 2.32 | Third-Party must have a data flow diagram for ARS engagement. |
| 2.33 | Third-Party must have a documented media disposal process. |
| 2.34 | If Third-Party is using mobile devices to access, process, store, and/or transmit ARS data then those mobile devices should be managed by a mobile device management (MDM) solution. |
| 2.35 | Third-Party must have an IT Security organization in place. The role of this team will be to perform IT risk assessments, internal audits, supporting external audits, maintain and monitor security metrics, reporting security posture to higher management etc. |
| 2.36 | Third-Party must ensure that a Disaster Recovery Plan (DRP) is documented and at least annually tested. |

## 3. PHYSICAL SECURITY REQUIREMENTS

**Applicability:** The physical security requirements are applicable to third-parties that process, access, or stores (logically or physically) ARS Confidential Information or Personal Data, ARS Highly Confidential Information or Sensitive Personal Data, Controlled Data or if the Third-Party has a direct network connection to the ARS managed network.

| Physical Security Requirements | |
|---|---|
| 3.1 | Third-Party must ensure that all facilities used to access, process, transmit, and/or store ARS data, have badge readers, security cameras, security guard and mantrap on all entry & exit points to ensure physical access is restricted to authorized personnel. |
| 3.2 | Third-Party must ensure that all servers and network equipment used to store and/or access ARS data shall be kept in a secure room with the proper controls in place. |
| 3.3 | Third-Party must retain security camera recordings for at least 30 days. |
| 3.4 | Third-Party must have/issue an identification badges for all employees, contractors, and visitors and delineate full time employees from contractors and visitors. |
| 3.5 | If applicable, third-party must ensure that all physical documents that contain ARS data/information shall be kept in a locked office, cabinet, or other location which is locked, and access restricted to authorized personnel only. |
| 3.6 | Third-Party must ensure to have a mechanism in place to notify, investigate, and address potential physical security incidents such as physical intrusion or a stolen asset. |
| 3.7 | Third-Party must ensure that all facilities used to access, process, transmit, and/or store ARS data are staffed 24x7x365 and if not, alarms should be installed for off-hour access monitoring. |
| 3.8 | Third-Party must ensure if a facility used to access, process, transmit, and/or store ARS data are not shared with other occupants (e.g.co-located data center). If it is shared, then protective mechanisms should be implemented between occupants to prevent unauthorized access to their organization's physical equipment. |
| 3.9 | Third-Party must ensure that physical access rights should be reviewed on an annual basis (at a and updated as needed to ensure physical access to all facilities used to access, process, transmit, and/or minimum) store ARS data is restricted to authorized personnel. |

## 4. SOFTWARE DEVELOPMENT

**Applicability:** The software development requirements are applicable to third parties that develop software specific to ARS 's needs or hosts applications that Process ARS Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Information.

| Software Developments Requirements | |
|---|---|
| 4.1 | Third-Party must ensure to have Software Development life cycle process documented and communicated to all employees and train them accordingly. |
| 4.2 | Third-Party must ensure to provide proper training to software developers based on their role. |
| 4.3 | Third-Party must ensure that all confirmed critical/high vulnerabilities (mediums and low depending on impact) found during testing shall be remediated and retested within 30 days of identification and prior to moving code to production |
| 4.4 | Third-Party must ensure that any software developed for ARS shall not contain any proprietary or open-source code developed or sold by an entity other than the contracting third-party unless approved by ARS |
| 4.5 | Third-Party must ensure that all software delivered to ARS shall be free of defects/vulnerabilities |
| 4.6 | Third-Party must ensure that if the third-party hosted application undergoes Significant Changes or Enhancements, ARS has the option to perform a technical penetration test (manual and/or automated) prior to the changes being implemented in production. |
| 4.7 | Third-Party must ensure that all third-party hosted applications shall be reassessed every two years. |
| 4.8 | Third-Party must ensure to have a designated application security representative that acts as the primary liaison between the Third-Party and ARS in matters related to secure application development, ensuring that their team following all ARS requirements for secure application development and provide requested evidence as per the request |

| | |
|---|---|
| 4.10 | Third-Party must have a secure design requirement documented & defined in collaboration with the ARS application owner and other key stakeholders. |
| 4.11 | Third-Party must ensure to have proper backup of code on a regular basis. |
| 4.12 | Third-Party must ensure that application development shall take place in a secured development environment. |
| 4.13 | Third-Party must ensure to perform Static Application Security Testing (SAST) & Dynamic Application Security Testing (DAST) on the code & application. |
| 4.14 | Third-Party must ensure to perform security design review to verify required security features and functionality |

## 5.CLOUD SECURITY

**Applicability:** The cloud security requirements are applicable to the third-party that host a cloud computing application in a SAAS, PAAS, IAAS, DRAAS etc. environment) that processes ARS Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data, or the third-party provides a cloud computing platform that allows ARS to develop, run, or manage applications, or the third-party is responsible for the management of virtual machine image and/or hypervisor.

| Cloud Security Requirements | |
|---|---|
| 5.1 | Third-Party must ensure that root/administrator access to the management console shall require multifactor authentication. |
| 5.2 | Third-Party must ensure a dedicated secure network, which shall be separate from customer production infrastructure, leveraged to provide management access to the cloud infrastructure. |
| 5.3 | Third-Party must ensure to store all cloud & account activities logs into a central log aggregation tool and they must have the ability to provide logs which are specific to the instances used for ARS |
| 5.4 | Third-Party must have a backup process for cloud VPC and a periodic restoration testing process. |
| 5.5 | Third-Party must ensure to retain the original structure and format of data residing within the cloud application for easy movement to another cloud solution/cloud service provider. |
| 5.6 | In cloud environment, Third-Party must ensure to encrypt ARS data at rest and control in place to protect encryption keys. |
| 5.7 | Third-Party must have an access management control for their cloud application & VPC. |
| 5.8 | Third-Party must have a cyber incident management process for their cloud application & VPC. |
| 5.9 | Third-Party must have a patch management process for their cloud application & VPC. |
| 5.10 | Third-Party must vault root/administrator account credentials. |
| 5.11 | Third-Party must ensure that web application/network vulnerability assessment or penetration test shall be performed for their cloud application & VPC at least annually. |
| 5.12 | Third-Party must implement web application firewall (WAF) for their cloud application. |
| 5.13 | Third-Party must have a control in place for monitoring configuration drift. |

## 6. DATA CENTRE SECURITY

**Applicability:** The data center security requirements are applicable to third-parties which provides data center facility services.

| Additional Data Center Security Requirements | |
|---|---|
| 6.1 | Third-Party must ensure to have proper physical security controls in place at their data center. |
| 6.2 | Third-Party must ensure that all assets containing ARS data shall be caged off physically from the rest of the data center and have physical security control in place to access those assets. |
| 6.3 | Third-Party must ensure to have an access management process of granting access to data center. They must store all access & user logs for at least 1 year and review them on a regular basis. |
| 6.4 | Third-Party must ensure that server rooms shall not be used for storage and shall be clear of all unnecessary equipment and material not in use. |
| 6.5 | Third-Party must ensure to have detective monitoring and controls implemented to mitigate the risk of overhead water sources impacting the IT equipment. |
| 6.6 | Third-Party must ensure that all data centers shall have a fire suppression system and all data center workers will be trained in control and storage of combustible materials and on the correct processes to follow when detecting a fire. |
| 6.7 | Third-Party must ensure that all computer devices are connected to surge protectors to protect them against spikes and surges in the electrical power supply. |
| 6.8 | Third-Party must ensure that backup power supply is available in the form of local generator(s). |
| 6.9 | Third-Party must ensure to have Emergency lighting, powered by a supply other than the main power, shall be |
| 6.10 | Third-Party must ensure that data center have a system in place to control and monitor temperature and humidity, air conditioning system to control air quality and minimize contamination. |
| 6.11 | Third-Party must ensure that data center shall have air conditioning systems with dust filtration systems by separating zones for standard working areas, and areas containing equipment such as server rooms. |
| 6.12 | Third-Party must ensure that server rooms shall have positive pressurization to minimize contaminants entering |
| 6.13 | Third-Party must ensure to have a process in place for scheduled testing and maintenance of all critical data center infrastructure including security, power & environmental systems. |
| 6.14 | Third-Party must ensure that critical data center infrastructure including power & environmental systems shall be engineered to function through an operational interruption. The design shall be a minimum of N+1 |
| 6.15 | Third-Party must ensure that all ARS equipment shall be properly mounted in appropriately sized racks which are ground and/or ceiling mounted in accordance with local earthquake guidelines. |
| 6.16 | Third-Party must ensure to have process in place for a movement of equipment. |
| 6.17 | Third-Party must ensure to have a documented equipment or media delivery or handling process. |
| 6.18 | Third-Party must ensure to have a DRP documented & tested. |
| 6.19 | Third-Party must ensure that all ARS equipment shall be completely network segregated from non-ARS parts of the data center. |

## 7. DIRECT NETWORK CONNECTIVITY SECURITY

**Applicability:** The direct network connectivity security requirements are applicable to third-parties that have a ARS Trusted Third-Party network connection.

| Direct Network Connectivity Security Requirements | |
|---|---|
| 7.1 | Third-Party shall use only ARS managed network devices to connect to the Trusted Third-Party connection. ARS requires out of band connectivity to the remote device for administration. |
| 7.2 | Third-Party shall implement a firewall between the third-party parent network and the Trusted Third-Party network. |
| 7.3 | Third-Party shall remediate all critical or high vulnerabilities within 30 days of notification by ARS |
| 7.4 | Third-Party must ensure that all internet traffic shall be directed to a ARS managed external proxy |
| 7.5 | Third-Party must ensure that remote access to the Trusted Third-Party network is only allowed through the ARS Virtual Private Network (VPN) hub infrastructure with two-factor authentication. |

| | |
|---|---|
| 7.6 | Third-Party must ensure that ARS managed network equipment shall be housed in a caged environment and/or be physically separated from the Third-Party equipment. |
| 7.7 | Third-Party must ensure to have a physical security control in place on ARS managed network equipment |
| 7.8 | Third-Party shall ensure that all wireless deployments on Trusted Third-Party networks must follow the ARS Third-Party network change request process and are configured/managed by ARS |
| 7.9 | Third-Party must ensure that all unused switch ports shall be disabled on network equipment. In addition, all new connection requests shall be submitted to ARS |

## 8. PRODUCT SECURITY

**Applicability:** Product security requirements are applicable if the third-party provides a product, component or service that includes or supports the following: software, firmware, and/or complex hardware (i.e. logic bearing device); designed to be operated in networked environment (i.e. provides a communication interface); USB/portable media access (e.g. CD/DVD/ext. disk); remote access (e.g. remote desktop protocol); services that include a software or networked component.

| Product Security Requirements | |
|---|---|
| 8.1 | Third-Party must ensure to have a documented product security policy that mandates requirements for reasonable industry specific measures to protect the products your company manufactures. |
| 8.2 | Third-Party must ensure to identify a product security leader and enterprise security architects in the execution of the product security program and resolution of cyber threats. |
| 8.3 | Third-Party must ensure to perform a Static Application Security Test (SAST) & Dynamic Application Security Test (DAST) on the product & software/firmware accordingly. |
| 8.4 | Third-Party must ensure that developer verify the integrity of software and firmware components. |
| 8.5 | Third-Party must ensure that proper testing will be performed on the open-source software or 3rd party components if they are included in the component ARS is purchasing. |
| 8.6 | Third-Party must ensure to have a proper authentication and authorization controls in place if the component is capable, which includes access & password management. |
| 8.7 | Third-Party must ensure to have a control in place if the component have remote access capability. Which includes encrypting the connections, limit the connection, etc. |
| 8.8 | Third-Party must ensure that if component have an interface/port to connect to portable storage devices then it should have controls in place to protect and have a documentation for connecting. |
| 8.9 | Third-Party must ensure to have capability to store & retain all type of logs for 180 days and make sure no one can tamper the logs. |
| 8.10 | Third-Party must ensure to have a product security incident response policy. Also, in future if Third Party identifies any cyber breach related to the product, then your organization must inform Security team |
| 8.11 | Third-Party must ensure to have product patch management process in place. |
| 8.12 | If applicable, Third-Party must ensure to have cyber-security certifications (example security by design with CMMI for development (v1.3), Wurldtech Achilles Communication Certifications, Wurldtech APC (IEC 62443-2-4) |
| 8.13 | Third-Party must ensure to have a product cyber security awareness training and make sure all employees are trained accordingly. |
| 8.14 | Third-Party must ensure to perform periodic security reviews and/or on-site audits/assessments of their suppliers/contractors if they work along with your organization in developing this component and they must comply with ARS product requirement. |
| 8.15 | Third-Party must ensure that services or capabilities that are not required to implement in the product functionality by default are disabled or require authentication. |
| 8.16 | Third-Party must perform penetration testing on the component(s) that ARS is purchasing. |

| | |
|---|---|
| 8.17 | Third-Party must ensure that product will comply with wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11) if the product incorporated with wireless technology. |
| 8.18 | Third-Party must ensure that they follow cryptographic controls to encrypt ARS data on the product and comply with NIST Special Publication 800-131A. |
| 8.19 | Third-Party must ensure to have a product vulnerability management process. |
| 8.20 | Third-Party must ensure that all software been digitally signed to ensure its integrity. |
| 8.21 | Third-Party must have a documented secure development life cycle standard in place. |
| 8.22 | Third-Party must develop a plan that identifies the applicable software development lifecycle objectives and customer/regulatory cybersecurity requirements. |
| 8.23 | Third-Party must ensure that the component that ARS is purchasing undergone a threat modeling exercise to assess and document the components inherent security risks. |
| 8.24 | Third-Party must have security architecture been developed and documented for the component that ARS is purchasing. |
| 8.25 | Third-Party must ensure that security verification and validation plan been developed & documented. |
| 8.26 | Third-Party must ensure that a digital obsolescence and end-of-life strategy been developed and documented. |
| 8.27 | Third-Party must have a continued deployment compliance plan been developed which includes the schedule and scope of reoccurring validation. |

## 9. RESILIENCY SECURITY REQUIREMENTS

**Applicability:** The resiliency security requirements are applicable to third parties that process, access, or stores (logically or physically) ARS Highly Confidential Information or Sensitive Personal Data, Controlled Data, if the supplier is a sole source or single source manufacturer of products, components, or materials for ARS where the supplier has a critical or high impact on operations/production of critical products.

| Resiliency Security Requirements | |
|---|---|
| 9.1 | Third-Party must have an information security incident management plan in place. |
| 9.2 | Third-Party must identify a stakeholder and assign roles & responsibilities to staff for carrying out the activities described in the security incident management plan. |
| 9.3 | Third-Party must have a process in place to escalate/communicate to stakeholders/effected parties about incident. |
| 9.4 | Third-Party must have management oversight of the performance on incident management activities and performance of the external dependency activities. |
| 9.5 | Third-Party must have service continuity plans in place. |
| 9.6 | Third-Party must have mechanisms in place to achieve resilience requirements in normal and adverse situations. |
| 9.7 | Third-Party must have a documented resilience requirements for external dependencies/relationships management. |
| 9.8 | Third-Party must have a process to identify, analyze and manage the risk arising from external dependency/relationship management |
| 9.9 | Third-Party must identify infrastructure providers on which the critical service depends. |
| 9.10 | Third-Party must have external dependency/relationship management activities reviewed periodically and measured to ensure they are effective, producing the intended results and adhering to the plan. |
| 9.11 | Third-Party must ensure to identify a resource to monitor threat and trained to communicate threat information for respective parties (internal/external) |

## 10. OPERATIONAL TECHNOLOGY (O.T.)/MANUFACTURING SECURITY REQUIREMENTS

**Applicability:** The O.T./Manufacturing security requirements are applicable to third-parties that manufactures products, components or materials for ARS ; excluding Commercial Off-the-Shelf (COTS) items, low cost and high-volume commodity items, and commercially available raw materials.

| Operational Technology Security Requirements | |
|---|---|
| 10.1 | Third-Party must ensure that all hardware and software assets used in their manufacturing environment are centrally managed and protected by the firewall. |
| 10.2 | Third-Party must contain all manufacturing assets in a locked facility or one that is badge access controlled. |
| 10.3 | Third-Party must ensure that all assets, software & firmware in their manufacturing environment are licensed and periodically scanned for malware & update to date with security patches/updates. |
| 10.4 | Third-Party must have a process in place to manage removable media such as USB devices, external hard drives, floppy disks, or compact disks. |
| 10.5 | Third-Party must have access management & password security controls in place for accessing assets in manufacturing environment. |
| 10.6 | Third-Party must ensure that all remote network connections to devices/equipment within their manufacturing environment are encrypted using AES 128, 192, or 256. |
| 10.7 | Third-Party must have a firewall restriction in place to limit remote connections to authorized endpoints only. |
| 10.8 | Third-Party must have a documented media disposal process in place. |
| 10.9 | Third-Party must monitor all assets in manufacturing environment for abnormal/malicious activity. |
| 10.10 | Third-Party must have a document incident management plan in place that covers their manufacturing environment. |
| 10.11 | Third-Party must have a process in place to inform ARS if have any data breach or other incidents within 72 hrs. |
| 10.12 | Third-Party have a documented BCP/DRP process for manufacturing environment. |
| 10.13 | Third-Party must have at least one manufacturing site that could be leveraged in the event the primary manufacturing site is adversely impacted due to a cyber incident. |
| 10.14 | Third-Party must capture and retain backups of manufacturing system software and firmware assets where possible. |
| 10.15 | Third-Party must have a document change management process for their manufacturing environment. |
| 10.16 | Third-Party must ensure to document the list of all the 3rd party software, firmware, or hardware used in their manufacturing environment |
| 10.17 | Third-Party must ensure to manage and periodically review the 3rd parties that have remote access to any assets within their manufacturing environment. |