RESIDEO

Contractor Information Security Addendum

September 2021

Contents

1. General Statement 1
2. Recognized Industry Standards 2
3. Definitions 2
4. Information Security Program 3
5. Human Resources Security 3
6. Business Continuity Management 4
7. Compliance and Audit 4
8. IT Security Operations 5
9. Access Management 6
10. Data Security 6
11. Network Security 7
12. Security Incident Management 8
13. Physical and Environmental Security 8
14. Additional Requirements for Resideo Product and Service Components 9

1. General Statement

1.1. This Resideo Contractor Information Security Addendum (the “**Addendum**”) lists the technical and organizational security measures and controls that the Contractor must apply when (to extent applicable to the scope of Service performed by the Contractor under the Agreement).

1.1.1. accessing Resideo or Resideo's customers' Facilities, Networks and/or Information Systems,

1.1.2. processing (including accessing, viewing, exchanging and/or storing) Sensitive Information, or

1.1.3. the Contractor provides Services that will form part of and/or directly support any products or services that Resideo makes available to its customers, partners, users and/or members of the public.

1.2. Notwithstanding anything to the contrary anywhere in the Agreement or this Addendum, Resideo acknowledges and agrees that the technical and organizational security measures and controls herein will be implemented to ensure a level of security appropriate to the risks of Sensitive Information maintained by Contractor, and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Services as well as the risk of harm to Resideo.

1.3. The Contractor is responsible for compliance with this Addendum by its Personnel, including ensuring that all Personnel are bound by contractual terms materially consistent with the requirements of this Addendum. Additional security compliance requirements may be specified and agreed in the Agreement.

1.4. In the event of any conflict or inconsistency between the terms of this Addendum and the Agreement and unless not otherwise explicitly stated in the Agreement, this Addendum shall prevail to the extent required to resolve such conflict or inconsistency.

1.5. Resideo may update this Addendum from time to time by publishing a new version at https://www.resideo.com/us/en/corporate/Suppliers and unless specifically stated otherwise in the Agreement the latest version as published shall apply once it has been formally agreed between the parties vide an amendment

2. Recognized Industry Standards

2.1. The following frameworks were used to develop this Addendum and they represent "recognized industry standards" for the purposes of this Addendum. Other recognized industry standards may also be relied on by the Contractor, where appropriate, and are referred to throughout this Addendum.

2.1.1. ISO/IEC 27001 Information Security Management

2.1.2. NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

2.1.3. ENISA ICT Procurement Security Guide for Electronic Communications Service Providers

2.1.4. AICPA 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

3. Definitions

Capitalized terms used in this Addendum have the same meaning as set out in the Agreement. Where the Agreement does not define a capitalized term used in this Addendum, that term has the meaning set out below:

“**Agreement**” means an agreement between Resideo and a Contractor ("*References to "Contractor" in this Exhibit are references to Resideo's contractual counterparty in the Agreement (where such party may be referred to as "Supplier", "Partner" or similar")* under which (a) Contractor performs Services for Resideo and/or (b) Contractor is provided access to Resideo Facilities, Network(s), Information Systems and/or Sensitive Information.

“Applications” means middleware, databases, applications, web portals, mobile applications and other software that are used as part of the Services.

“Asset” means any tangible and intangible Resideo-owned item for which a Contractor has responsibility.

“Cloud Computing” means model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that is used as part of the Services.

“Computer” means any desktop computer, laptop computer, mobile device (e.g., cellular phone, smartphone, tablet), server and/or storage device that (i) is used as part of the Services, (ii) may be used to access a Network or Cloud Computing, and/or (iii) may process Sensitive Information.

“**Contractor**” means an entity (including its Personnel) that performs Services for Resideo under the Agreement and/or which is granted access to Resideo Facilities, Networks, Information Systems and/or Sensitive Information.

“Electronic Media” means hard disk, solid state disk, DVD/CD, tape or any other form of media that can store electronic information.

“Facilities” means any offices, data centers and other locations (whether owned or managed by Resideo, a Resideo customer, Contractor or a third-party or any remote working locations which are not owned/managed by the Contractor) from which Sensitive Information, Information Systems or Networks may be accessed. References in this document to (i) “Resideo Facilities” shall be deemed to include facilities of Resideo customers, and (ii) “Contractor Facilities” shall be deemed to include third-party facilities used by Contractor.

“Information Systems” means any Contractor's system (including but not limited to development, test, stage and production systems, storage/backup systems etc.), that (a) is used as part of the Services and/or (b) may process Sensitive Information.

“Network” means any Resideo networks to which Contractor is provided access in connection with the performance of Services under the Agreement and/or any Contractor networks that are used to process Sensitive Information or to access Information Systems.

“Personnel” means all Contractor employees, contractors, sub-contractors and agents who are provided access to Resideo Facilities, Networks, Information Systems and/or Sensitive Information.

“Security Incident” means (a) unauthorized access to Sensitive Information or Information Systems, or (b) the loss of confidentiality, integrity or availability of any Service and includes a Security Breach (where defined in the Agreement). For clarity, events that do not and cannot result in unauthorized access, use, disclosure, modification or destruction of Sensitive Information, are not considered a Security Incident. For illustrative purposes only, this includes a) pings on Contractor’s firewall; b) port scans; c) attempts to log on to a system or enter a database with an invalid password or username; d) denial-of-service attacks that do not result in a Service being taken dysfunctional.

“Sensitive Information” means all Resideo sensitive information to which Contractor may be provided access in connection with the performance of the Services, including without limitation personal data (as defined in applicable privacy laws and including Resideo Personal Data where defined in the Agreement); Resideo's Confidential Information (where defined in the Agreement); intellectual property; source code; passwords; information concerning Resideo’s employees, customers, Contractors or partners; any data stored in or provided from the Information Systems of Resideo or its customers, other Contractors or partners; and any other Sensitive Information as defined in the Agreement. References in this document to “Sensitive Information” shall be deemed to include Sensitive Information of Resideo employees, customers, Contractors or partners to which Contractor is provided access in connection with providing Services. With the exception of Personal Data, “Sensitive Information” shall exclude any information if Contractor can demonstrate that the information: (a) is or becomes generally known to the public not as a result of a disclosure by Contractor; (b) is rightfully in the possession of the Contractor prior to disclosure by Resideo and is not accompanied by a duty of confidentiality; (c) is received by Contractor in good faith and without restriction from a third party and is not accompanied by a duty of confidentiality; or (d) can be shown with evidence it was developed independently by or on behalf of the Contractor without the use of any Sensitive Information of Resideo.

“**Services**” means the work to be performed or deliverables to be delivered by Contractor for Resideo as specified in the Agreement and which may include but not limited to the manufacture, delivery and/or support (as relevant) of software, products, services and/or other deliverables.

4. Information Security Program

4.1. Contractor must have clearly defined the information security roles, responsibilities and accountability within its organization.

4.2. Contractor must publish and maintain formal and appropriate written information security policies. Information security policies must be approved by management and its Personnel must be appropriately informed of them.

4.3. Contractor must classify and label Sensitive Information in accordance with its information classification scheme.

4.4. Contractor must implement appropriate security processes for managing Contractors and subcontractors throughout the business relationship lifecycle.

4.5. Contractor must maintain an inventory of Assets and business-critical Information Systems that are used as part of the Services. The inventory must be accurate, up to date with responsible Contractor Personnel assigned to each Asset and relevant Information System.

4.6. Contractor must maintain a complete list of all Personnel granted permission to access Resideo Facilities, Information Systems, Sensitive Information, Networks and Applications, including their geographic location. Personnel access must be reviewed at least twice per calendar year, and access promptly revoked when no longer necessary for the relevant job function.

4.7. Contractor must establish and maintain an appropriate risk management program to address probable and/or actual validated internal and external threats that could cause a Security Incident.

4.8. Contractor must periodically (not less than once per calendar year) review the policies and procedures it maintains pursuant to this section (Information Security Program) to ensure that they meet the requirements of the Agreement and remain appropriate and effective.

5. Human Resources Security

5.1. Contractor must perform its own standard background checks, consistent with its own policies and subject to local laws and regulations, for all Personnel. The level of verification performed must be proportional to risk correlated to their roles within the Contractor's organization.

5.2. Contractor Personnel are required to agree, in writing, to abide by Contractor’s security policies and procedures.

5.3. Contractor must have a comprehensive security awareness program for all Personnel that encompasses education, training, protection of Sensitive Information and updates for security policies and procedures. Training must be provided at time of hiring and repeated at regular intervals thereafter (no less than every year).

5.4. Contractor must have formal disciplinary processes in place for Personnel and take appropriate action against Personnel who violate Contractor’s policies and procedures, based upon the nature and gravity of the violation.

5.5. Timely de-provisioning, revocation or modification of relevant Contractor's Personnel access to Information Systems, Networks and Applications must be implemented upon any change in status of Contractor's Personnel.

Any change in status is intended to include termination of employment, contract or agreement, change of employment or transfer within the organization.

5.6. Subject to the Agreement, Contractor is authorized to use subcontractors for the provision of the Services if they are contractually bound to comply with obligations consistent with those set forth in the Agreement and this Addendum. Contractor must maintain a list of its subcontractors and the country/countries to which Sensitive Information may be transferred to or accessed from and will provide that list to Resideo upon written request (or as otherwise set out in the Agreement). Resideo may reject the use of any subcontractor in accordance with the terms of the Agreement.

5.7. Contractor must ensure its Personnel has the appropriate rights to work documentation as necessary and required to enable the Contractor's Personnel to provide the Services.

6. Business Continuity Management

6.1. Contractor must have a disaster recovery ("**DR**") program and maintain a documented organizational business continuity plan ("**BCP**"). The DR program and BCP must be designed to ensure that Contractor can continue to function through operational interruption and continue to provide Services, as specified in the Agreement. Contractor must provide Resideo written summaries of its DR program and BCP upon written request.

6.2. Contractor must ensure that the scope of the BCP covers all Contractor Facilities, Personnel, Applications, Networks and Information Systems that are used as part of the Services.

6.3. The BCP must be tested on a regular basis (at minimum, once per calendar year). Contractor must document the results. On written request, Contractor must provide documentation for Resideo's review to confirm that tests are being performed.

6.4. Contractor must promptly notify and report the potential impact to Resideo when the DR plan is executed.

7. Compliance and Audit

7.1. Contractor must inform Resideo if legislation applicable to the Contractor could prevent the Contractor from fulfilling the obligations relating to treatment of Sensitive Information.

7.2. In the event Contractor processes Sensitive Information that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Contractor agrees to reasonably cooperate with Resideo to comply with such requirements, including negotiating in good faith additional agreements as required for such compliance.

7.3. Contractor must provide Resideo with the contact information of the person(s) Resideo may contact in relation to any information security and/or compliance issues.

7.4. If the Services involve the processing of payment card information, Contractor must maintain compliance with the current version of the Data Security Standards (DSS) from the Payment Card Industry Security Standards Council (PCI SSC) for as long as the Services are provided to Resideo. On request, Contractor will provide Resideo with the most recent PCI SSC "Attestation of Compliance" (AoC) reports prepared by a third-party PCI Qualified Security Assessor (QSA) for all Information Systems that Contractors uses to process payment card information.

7.5. If the Services involve Protected Health Information ("**PHI**") subject to the U.S. Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated under that Act (collectively, "**HIPAA**"), the Contractor must maintain compliance with HIPAA. On request, Contractor must provide Resideo reasonable assurance that Contractor (and any third parties used by the Contractor for processing PHI) maintains sufficient technical and organizational controls to comply with HIPAA requirements. This assurance may include audits and assessments from a qualified third-party and/or completion of a questionnaire with sufficient evidence to support Contractor's compliance.

7.6. Upon request, Contractor shall share reasonable information concerning the independent third-party information security audit reports (i.e. SSAE 16, ISO 27001) that it has commissioned in respect of the Information Systems (if any) used for delivering the Service.

7.7. Subject to the Agreement, Resideo may perform security assessments, at most once yearly, to verify compliance with this Addendum. Resideo will provide reasonable prior written notice to the Contractor of a verification audit and ensure the audit is performed during Contractor's normal business hours, and with minimal disruption to the Contractor's business operations. Resideo may also request, on an annual basis, that Contractor completes a reasonable questionnaire concerning its compliance with this Addendum and its security practices to enable Resideo to assess the Contractor's compliance. If as part of this process Resideo, acting reasonably, identifies any non-compliance, Contractor shall remedy such non-compliance promptly. Audit right does not include the right to install audit tools, the right to conduct ethical hacking, penetration testing or vulnerability testing of the Contractor's systems or network; and (i) Resideo and its auditors shall not be entitled to audit (a) data or information of other customers of Contractor, (b) any Contractor proprietary data, including cost information or personnel data, or (c) any other Contractor Confidential Information that is not relevant for the purposes of the audit; and in case of any audit is conducted remotely, Resideo or its affiliate's shall not record or capture any sound, images, etc. shared during the course of the audit and shall not access or retain any documented information in excess of what it would in a traditional physical on-site assessment.

8. IT Security Operations

8.1. Contractor's Information Systems, Network devices, Computers and Applications must be configured and deployed using a secure baseline (hardened) for security operational parameters and to the extent technically feasible all accounts, software, services and ports that are not in use must be disabled. All default passwords must be changed to the extent technically feasible.

8.2. Contractor must return without undue delay all Assets to Resideo upon request.

8.3. Contractor must implement appropriate controls within its environment to terminate inactive sessions and restrict the connection times of idle/inactive sessions on Information Systems, Applications and Network devices.

8.4. System clocks must be synchronized to a trusted time server source, maintaining accurate and synchronized time/time zone on all Information Systems, Computers and Network devices and ensuring log files have consistent time stamp information recorded.

8.5. To the extent applicable, Contractor must have implemented and documented a secure software development lifecycle program with version control, traceability of code and consistent change management that includes appropriate security requirements (including risk assessment, threat modeling, security design review, static code analysis, security testing and dynamic application vulnerability scanning) for all Contractor-developed Applications and source code that Contractor uses as part of providing the Services.

8.6. Prior to implementation of new Applications and Information Systems, Contractor must carry out a security review process to validate the security of the service design stage, in order to identify potential security issues ahead of deployment.

8.7. Contractor must perform appropriate security assessments, scans and testing of its Information Systems, Networks, Computers and Applications at planned intervals, at least once per calendar year, to verify compliance with its security policies and standards.

8.8. Contractor must maintain documented change management procedures that provide a consistent approach for controlling and identifying configuration changes for Information Systems, Computers, Applications and Network devices.

8.9. If mobile devices are used in the delivery of Services to Resideo, those must be managed using centralized mobile device management software that has the capability to remotely lock and wipe lost/stolen mobile devices.

8.10. The Contractor must perform periodic authenticated and unauthenticated vulnerability scans for Applications, Information Systems, Computers and Networks (including, where relevant, regular penetration network testing, static code analysis and dynamic Application vulnerability scanning).

8.11. Contractor must track information from technology vendors and other relevant sources in relation to technical vulnerabilities of operating systems, Applications, and Network devices and must promptly evaluate exposure to reported and known vulnerabilities to ensure that appropriate measures are taken to address any potential risks of a Security Incident occurring.

8.12. Contractor must promptly apply patches for all operating systems, Applications and Network devices according to an appropriate and documented vulnerability and patch management process that requires patches be applied in a consistent, standardized manner and prioritized based on criticality and risk. If a security patch cannot be promptly applied due the need for appropriate prior testing, then effective risk mitigation controls to the extent reasonably possible must be implemented until such time that patches can be applied.

8.13. Where reasonably feasible, Computers must be configured to automatically receive operating system patches and updates from a centralized service that manages and distributes updates.

8.14. Contractor must use software to prevent, detect and remove viruses, malware and similar types of malicious code ("**AV Software**"). Such AV Software must provide automated virus/malware signature updates and detect if it has been disabled on particular Computers and/or is not receiving regular such updates.

8.15. The Contractor must use AV Software to automatically scan all e-mail attachments from/to its managed email accounts that are sent to or received from external sources. Attachments that are identified as containing malicious code must be removed.

8.16. Contractor must maintain logs from Information Systems, Network devices and Applications for a minimum period of 90 days (subject to local law) and store log files on a centralized logging server. Logs should be sufficiently detailed in order to assist in the identification of the source of an issue and enable a sequence of events to be recreated.

8.17. Contractor must ensure that the logs referred to in this Addendum have record date, time and source location (IP address/hostname) for all access attempts and also capture system and network security event information, alerts, failures, events and errors. Contractor must ensure that the integrity of such log files is maintained and protected from tampering by restricting access to systems that store such log files.

8.18. If Contractor uses Cloud Computing as part of the Services, the Contractor shall ensure that such Cloud Computing has at minimum the same level of security as it is described in this Addendum.

9. Access Management

9.1. Contractor must have user account management procedures to support the secure creation, amendment and deletion of accounts on Information Systems, Network devices and Applications.

9.2. The procedures must include processes for ensuring that Information Systems, Applications and Network device owners authorize all new user account requests and identification of redundant accounts.

9.3. Contractor Personnel must not share account credentials. All user accounts must be attributable to individuals (i.e. every account will have a unique login identifier and password).

9.4. Access controls must be implemented for Information Systems, Networks and Applications that verify the identity of all users and restrict access to authorized users with "need to know" principle.

9.5. Access controls must use a role-based access model and differentiate access levels for end-users and privileged access (e.g. systems administrators).

9.6. Approvals for access requests must have appropriate segregation of duties, e.g. different Personnel must perform the access authorization and access administration roles.

9.7. Access lists for Information Systems, Network devices and Applications must be reviewed on a regular basis and access immediately removed when no longer required.

9.8. Access to Resideo Sensitive Data, Information Systems, Networks and Applications by Contractor Personnel is strictly limited to the performance of the Services, as specified in the Agreement.

9.9. Strong password practices must be implemented, including minimum password length and complexity requirements (e.g. no dictionary words, use a mix of alpha numeric characters etc.).

9.10. Passwords must have a defined expiration period corresponding to the password practices defined by all requirements for memorized secrets found in recognized industry standards (e.g. National Institute of Standards and Technology (NIST) Special Publication 800-53B).

9.11. Passwords must be distributed separately from account information, in a manner that ensures confidentiality of information.

9.12. Passwords must be encrypted when transmitted between Information Systems, Network devices and Applications.

9.13. To the extent applicable, Contractor must employ encryption and strong authentication mechanism such as hardware token-based authentication and multi-factor authentication for privileged access and remote access to critical Information Systems, Networks and Applications.

10. Data Security

10.1. Contractor must ensure Information Systems, Computers and Applications involved in the performance of the Services are backed up to online and/or offline storage. Backups must be tested in accordance with the Contractor's appropriate operational backup procedures.

10.2. Backup media leaving Contractor’s facility must be protected against unauthorized access, misuse or corruption during transportation. Sensitive Information stored on backup media must be encrypted using 128-bit or higher encryption.

10.3. Contractor must, before processing Sensitive Information, implement both at System and Sub-System levels technical and organizational security measures consistent with recognized industry standards and applicable privacy laws to protect Sensitive Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

10.4. When using a shared hardware environment to deliver the Services, Contractor must implement information protection measures throughout the information lifecycle to ensure that Sensitive Information is physically or logically separated.

10.5. Contractor must process Sensitive Information only for the purposes of performing the Services as specified in the Agreement and in compliance with this Addendum.

10.6. Sensitive Information stored on Contractor's Computers and external Electronic Media must be fully encrypted using encryption algorithms and key sizes set out in recognized industry standards (e.g. Federal Information Processing Standard Publication FIPS 140-2).

10.7. Sensitive Information may not be stored on mobile devices unless such mobile devices (including any media cards used) are encrypted using encryption algorithms and key sizes set out in generally accepted recognized industry standards (e.g. Federal Information Processing Standard Publication FIPS 140-2).

10.8. Contractor must, to the extent applicable, delete and securely destroy Sensitive Information upon Resideo's request, upon completion of Services or upon the termination of the Agreement (whichever is sooner). Upon the expiry or termination of the Services and if requested by Resideo, Contractor must make available to Resideo in a commonly used and agreed electronic format (including via appropriate self-service functionality available to Resideo via the Services) a copy of the Sensitive Information which Contractor processes at that time.

10.9. Electronic Media used in the delivery of Services to Resideo or that contain Resideo Sensitive Data and are defective must be sanitized before disposal or repurposing (or, where defective, physically destroyed), using a process that assures data deletion and prevents data from being reconstructed or read, as prescribed in a generally accepted recognized industry standards (e.g. NIST SP 800-88). Physical transfer of Electronic Media must include delivery tracking and accountability.

10.10. Sensitive Information must not be transmitted unencrypted over public networks. Encrypted protocols that protect the Sensitive Information as set out in generally approved industry standards (e.g., SSL, SFTP, TLS) must be used.

10.11. Where Services require Sensitive Information to be exchanged using e-mail, Transport Layer Security (TLS) between Resideo mail gateways and Contractor mail gateways must be used.

10.12. Contractor must ensure that its Personnel do not use personal email accounts to exchange or process Sensitive Information.

10.13. Contractor must not use Sensitive Information from production systems for development, testing or staging purposes unless specifically permitted in the Agreement.

10.14. Contractor must separate production systems from development and testing environments and maintain access controls to establish separation between development and operations Personnel, as well as other potentially conflicting roles.

10.15. Contractor must not use public cloud storage services not contractually covered by Contractor to process Sensitive Information, unless specifically permitted in the Agreement.

10.16. A clear desk policy must be enforced in areas where Sensitive Information is stored. Documents and/or physical media devices that contain Sensitive Information must be securely stored when not in use.

11. Network Security

11.1. Contractor must implement and maintain Network security infrastructure components such as firewalls, intrusion detection/prevention systems (IDS/IPS) and other security controls, providing detection, continuous monitoring, and restrictive network traffic flow to assist in limiting the impact of attacks.

11.2. Network traffic must be appropriately segregated, with routing and access controls separating traffic on internal Networks from public or other untrusted networks.

11.3. To the extent applicable to the scope of Services, Contractor must maintain a current Network diagram, with clearly identified critical environments, data flows and inventory of all interconnections and connections to external networks (including Resideo's Network, internet, extranet, telephone networks, wireless networks) not controlled by the Contractor. This includes maintaining and periodically updating relevant documentation.

11.4. To the extent applicable to the scope of Services, Network environments must be designed and configured to restrict connections between segments of different levels of trust (i.e., trusted and untrusted) Networks via boundary protection mechanisms (e.g. proxies, gateways, routers, firewalls) and reviewed at planned intervals, documenting the business justification for use of all services, protocols, and ports allowed, including rationale or compensating controls implemented for those protocols considered to be insecure.

11.5. To the extent applicable to the scope of Services, Remote access into the Contractor's Network must be approved and restricted to authorized Personnel only. Remote access must be controlled by secure access control protocols, encryption and authentication. Privileged remote access must have multi-factor authentication, when technically feasible.

11.6. Where applicable to the Services, if VPN access (either site-to-site or IPsec) is used to connect to Resideo Networks and Information Systems, Contractor must segregate Computers that remotely connect to Resideo (using either physical segregation or VLAN subnets) to prevent Sensitive Information, Networks and Information Systems from potentially being accessible or visible by other personnel on the Contractor Network.

11.7. To the extent permitted by law, Resideo reserves the right to monitor Contractor access to and use of Resideo Information Systems, Networks and Applications.

12. Security Incident Management

12.1. Contractor must have documented Security Incident procedures, enabling effective and orderly management of Security Incidents. The procedures must cover the reporting, analysis, monitoring and resolution of Security Incidents.

12.2. Contractor shall investigate each Security Incident promptly, determine its impact and take all necessary measures to resolve it and mitigate its effects to the extent reasonable possible. All confirmed Security Incidents must be classified, prioritized and documented.

12.3. Security Incidents should be handled by a dedicated security incident response team or Contractor Personnel who are trained in handling and assessing Security Incidents in order to ensure appropriate procedures are followed for the identification, collection, acquisition and preservation of information relating to Security Incidents.

12.4. Without prejudice to the Agreement, Contractor must promptly report confirmed Security Incidents of which they become aware (but at the latest within 24 hours or such timeframe as specified in the Agreement) to their business contacts at Resideo for the applicable Services impacted by the Security Incident and by sending an e-mail to cirt@resideo.com. Contractor shall provide all reasonably relevant information concerning each Security Incident to Resideo as it becomes available. Contractor shall provide all reasonable cooperation and assistance regarding the Security Incident to Resideo.

12.5. Other than to law enforcement, Contractor's service providers, its legal counsel, or as otherwise required by law or permitted under the Agreement, Contractor may not make or permit any public statements concerning Security Incidents involving Sensitive Information, Information Systems or Assets to a third-party without the written authorization of Resideo's Legal Department.

12.6. Unless prohibited by law, Contractor must promptly notify Resideo in the event the Contractor receives a request for access to Sensitive Information or Information Systems and follow Resideo's reasonable instruction concerning such request.

13. Physical and Environmental Security

13.1. Parties hereby acknowledge and agree that these provisions as stated hereunder shall not be directly applicable to the Contractor but to their third party contracted services in the event the Services are being performed from remote work locations which are not owned/managed by the Contractor.

13.2. Contractor must maintain a physical security plan to protect Contractor Facilities that contain Sensitive Information, that addresses internal and external threats to such Contractor Facilities. Plans must be reviewed and updated on at least an annual basis.

13.3. Contractor Facilities must have secure entry points that restrict access and protect against unauthorized access. Access to all Contractor Facilities must be limited to authorized personnel and approved visitors. All visitors must be logged and required to sign a visitor register.

13.4. Contractor personnel and authorized visitors must be issued identification cards. Visitor identification cards must be distinguishable from Contractor personnel identification.

13.5. Security guards, intrusion detection, and/or CCTV cameras should be used to monitor Contractor Facility entry points, loading and shipping docks, and public access areas.

13.6. Reception areas for Contractor Facilities should be manned by a receptionist or security guard. Out of hours access must be monitored, recorded and controlled. Logs detailing access must be stored for a period of at least 90 days.

13.7. Access cards and keys that provide access to secure areas in Contractor Facilities such as data centers must be monitored and limited to authorized personnel. Regular reviews of access rights must be performed.

13.8. Off-site removal of Information Systems, Computers and Network devices must be restricted, approved and authorized by Contractor's security departments.

13.9. Contractor Personnel are required to abide by Resideo's security requirements and direction when working at Resideo Facilities. The security measures employed at Resideo Facilities (e.g., use and placement of security cameras, use and placement of other physical and logical security controls) are Sensitive Information. Personnel may not photograph or otherwise record Resideo Facilities or Information Systems, unless required for the performance of Services.

13.10. Contractor Personnel may not access Resideo Computers, Information Systems or Networks unless access expressly authorized by Resideo personnel.

14. Contractor Product Security Requirements – Appendix A

Additional Requirements for Resideo Product and Service Components

Subject to the terms of the Agreement, if any part of the Services is intended to be incorporated into and/or directly support any product or service that Resideo makes available to its customers, partners, users and/or members of the public, Contractor shall comply with Contractor Product Security Requirements listed in Appendix A "Resideo Contractor Product Security Requirements)

Appendix A

RESIDEO

Contractor Product Security Requirements

September 2021

Contents

1. Product Lifecycle Requirements 10
2. Product Requirements 13
3. Product Cloud Requirements 15

1. Product Lifecycle Requirements

1.1. Risk Understanding - Contractor and Resideo agree to work together to understand and document the risks facing the application. This effort should identify the key risks to the important assets and functions provided by the application. Each of the topics listed in the requirements section should be considered. The Contractor will:

1.1.1. Document in a risk analysis any unmitigated risks identified in the threat model (see 1.3.4) and quantify them using CVSS Version 3.0 and deliver the risk analysis report.

1.1.2. Any risk identified during security test or static and dynamic code analyses will be documented and shared with Resideo.

1.2. Requirements - Based on the risks, Contractor and Resideo agree to work together to create detailed security requirements as a part of the specification of the software to be developed. Requirements may be satisfied by custom software, third party software, or the platform. The Contractor will:

1.2.1. Create and maintain a requirements document outlining the requirements of the product. This document should contain functional requirements as well as security control requirements.

1.2.2. All changes to security requirements should be confirmed ahead of time with Resideo.

1.3. Design – Contractor will

1.3.1. Create documentation that clearly explains the design for achieving each of the security requirements. In most cases, this documentation will describe security mechanisms, where the mechanisms fit into the architecture and all relevant design patterns to ensure their proper use. The design should clearly specify whether the support comes from custom software, third party software, or the platform.

1.3.2. Ensure integrity in the design of the product to assure that there is no unauthorized modification of the software or data. Industry standard mechanisms such as hashing, using referential integrity, resourcing locking and code signing, any combination of these techniques or other industry standard techniques can be used for providing the integrity.

1.3.3. Architect the software keeping the core secure software concepts in mind. Evidence of this awareness during the design phase will be required during audits. Formal definitions of these concepts are available from Resideo. The Core Secure Software Concepts are:

- Least privilege
- Separation of Duties
- Defense in Depth
- Fail Secure
- Economy of Mechanisms
- Complete Mediation
- Open Design
- Least Common Mechanisms
- Psychological Acceptability

- Weakest link
- Leveraging Existing Components

1.3.4. Perform a threat modeling activity to identify threats to the product. This activity will be based on a well-known industry accepted methodology such as Microsoft's STRIDE model or the usage of a tool such as Microsoft's Threat Modeling Tool 2016. The threat model should identify the total attack surface for the product, prioritize the threats, and identify appropriate security controls to mitigate the threat.

1.3.5. Share the threat model in the form of a document with Resideo Product Security representatives.

1.3.6. Perform an attack surface evaluation.

1.3.7. Design in controls for any threats prioritized in the risk analysis (see 1.1.1).

1.3.8. In the process of mitigating a security risk, make sure that the risk has been fully assessed and described in detail.

1.3.9. Share the solution of mitigating security risk in the form of a document with Resideo.

1.4. Implementation

1.4.1. Contractor shall ensure its employees ("Developer") follow a set of secure coding guidelines and use a set of common security control programming interfaces (such as the OWASP Enterprise Security API (ESAPI)).

1.4.2. Guidelines will indicate how code should be formatted, structured, and commented. Common security control programming interfaces will define how security controls must be called and how security controls will function.

1.4.3. All security-relevant code will be thoroughly commented.

1.4.4. All code will be reviewed by at least one other Developer against the security requirements and coding guideline before it is considered ready for unit testing.

1.4.5. All code shall be run through a code static analysis tool and a binary security scan tool.

1.4.6. The scan results of static code analysis tool and binary security scan should be shared with Resideo while providing product, software / firmware.

1.5. Security Analysis and Testing

1.5.1. Contractor will establish and maintain system testing policies, standards and procedures.

1.5.2. Contractor agrees to conduct at least annual vulnerability assessments and remediation of any issues or deficiencies discovered in the testing as required by this Agreement and, current applicable industry standards (including, but not limited to, ISO 27001 and PCI-DSS, as applicable). Contractor's obligations, as they relate to vulnerability scans, are further described in Section 1.7 review and test custom code to identify potential coding vulnerabilities in accordance with industry standard security practices such as OWASP. Evidence of this assessment and the remediation actions taken will be provided upon request. If unable to provide documented evidence, a warranty period of no less than one year will be provided by the Contractor.

1.5.3. Contractor will perform application security analysis and testing (also called "verification") according to the verification requirements of an agreed-upon standard (such as the OWASP Application Security Verification Standard (ASVS)).

1.5.4. Contractor will document verification findings according to the reporting requirements of the standard.

1.5.5. Contractor will provide the verification findings to Resideo.

1.5.6. All Products will be tested to ensure full functionality with then current industry recognized virus scanning software or as other directed by Resideo.

1.5.7. Contractor will ensure that all antivirus and malicious code protection mechanisms used to test Products prior to shipping are current, actively running, and correctly generating audit logs.

1.5.8. Contractor shall provide the security test report of third party or Contractor's own security test lab to Resideo Security representatives in accordance with Resideo's requirements while providing product, software / firmware.

1.6. Secure Deployment

1.6.1. Contractor agrees to provide secure configuration guidelines that fully describe all security relevant configuration options and their implications for the overall security of the software.

1.6.2. The guideline will include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured for security.

1.6.3. The default configuration of the software shall be secure ("secure by default"). Reconfiguration of the software or system to a less secure state shall require verifiable acknowledgment by the end user or other person doing the configuring to ensure that they have accepted the risk of the less-secure configuration.

1.6.4. The product, packaging, and instructions shall be designed and manufactured to prevent supply-chain attacks that could result in malware being installed undetectably in the product between the time it is shipped from the manufacturer and the time it is received by the customer. It shall also be designed and manufactured to prevent this attack once it has been installed or has entered service.

1.7. Vulnerability / Patch Management

1.7.1. Contractor will conduct quarterly network based and host vulnerability scans inclusive of all products. Test security modules and assess system attributes that allow threats to succeed such as poor password management, non-hardened infrastructure devices, such as, but not limited to, firewalls or switches that are exposed to unauthorized users. Where in-house expertise is lacked, the Contractor will engage third party security professionals to conduct such tests.

1.7.2. Contractor will collect input on vulnerabilities (within Contractor's source code as well as from all included third party code including open source) from varied sources including, but not limited to, periodic binary scans of their software and/or firmware, vulnerabilities databases (e.q. OWASP Top 10, NVDB, OSVDB, etc.), bug tracking lists, researchers and customers.

1.7.3. Contractor will analyze the applicability of the vulnerabilities.

1.7.4. Contractor will provide articulated descriptions of discovered vulnerabilities within 24 hours to Resideo.

1.7.5. In products that are already launched, Contractor will apply security patches for all applicable software and hardware devices per the timeliness policy below based on patch severity rating (CVSS 3.0):

- Critical – CVSS score of 9 and above in 7 days
- High - CVSS score of 7 - 8.9 in 30 days
- Medium - CVSS score of 4 – 6.9 in 90 days
- Low – CVSS score of 3.9 and below in 180 days

1.7.6. Any deviations to the timeframes defined above must be mutually agreed by the parties. Contractor's failure to correct a vulnerability in accordance with this Section will be considered a material breach of this Agreement.

1.8. Change Management

1.8.1. Contractor will employ change management/version control tools that provide for auditing of changes made to the software code.

1.8.2. Chain of custody will be maintained ensuring that each change to the software is authorized by Resideo designated personnel, transparent (Resideo personnel are informed of the exact changes made to the software) and verifiable (changes are linked to the authorization).

1.9. Product Security Incident response

1.9.1. Contractor will maintain procedures used for timely security incident responses and security incident escalation in the internal control framework to Resideo. Contractor's obligations shall include, but not be limited to, the following:

- Resideo shall be informed of any security incidents within 24 hours of discovery.
- Resideo shall be informed prior to any disclosure outside of Contractor.
- Maintaining agreed upon procedures for incident reporting, monitoring, and tracking of all security incidents until they are resolved.
- Maintaining calling rosters (points of contact) and escalation plans.
- Verifying third party contracts include procedures for reporting and managing security incidents.
- Maintaining process steps that prevent further loss and preserve the system for forensic analysis.
- Maintaining plans to isolate compromised systems from the network, but which do not turn off the devices.

1.9.2. Having documented procedures to be shared with Resideo upon request.

1.10. Miscellaneous

1.10.1. No diagnostic backdoors will be permitted, and all configuration ports shall be disclosed to Resideo and properly restricted.

1.10.2. All user interfaces and open network ports will be identified and have a detailed description of their use supplied to Resideo upon release of the product to Resideo.

1.11. Export Licenses

1.11.1. Contractor will identify to Resideo any/all aspects of the software that may be subject to export control or foreign trade data regulations.

2. Product Requirements

2.1. These requirements represent the minimum standard of security requirements that are required for any product delivered to Resideo. Product specifications from Resideo may have additional product-specific requirements.

2.2. Input Validation and Encoding

2.2.1. The requirements will specify the rules for canonicalizing, validating, and encoding each input to the application, whether from users, file systems, databases, directories, or external systems.

2.2.2. The default rule will be that all input is invalid unless it matches a detailed specification of what is allowed.

2.2.3. The requirements will specify the action to be taken when invalid input is received.

2.2.4. The application will not be susceptible to injection, overflow, tampering, or other corrupt input attacks.

2.3. Authentication, Session Management and System Requirements

2.3.1. Any provided interface into the product will be authenticated in the manner set forth below.

2.3.2. The requirements will specify how authentication credentials and session identifiers will be protected throughout their lifecycle. Requirements for all related functions, including forgotten passwords, changing passwords, remembering passwords, logout, and multiple logins, will be included.

2.3.3. Product will meet or exceed the password guidelines outlined in this section or in a specification set forth in this Agreement.

2.3.4. Product will contain anti-tampering and resistance controls.

2.3.5. Product will contain authenticity and anti-counterfeiting controls.

2.3.6. Implement and enforce the Resideo user credential and password complexity settings.

2.3.7. Disclosure: Passwords will not be disclosed to anyone other than the owner of the account.

2.3.8. Depending on the scope and complexity of the product the following system requirements apply:

- Hardware security support – if the product includes a master microcontroller unit, there shall be secure hardware storage (either separate or as part of the MCU internals) for safe storage of secret information such as a private key.
- Secure boot – if the product is a bootable device or participates in system boot-up either in standalone or embedded form, it shall be able to perform secure boot or verified boot.
- Device identity – if the product has a discrete component with a microcontroller it shall have the capability to host a tamper-resistant device identity in the form of a secret public key certificate that can be universally verified but cannot be removed from the device.
- Code signing – if the product includes a software/firmware component, the software code base shall enable verification of code authenticity using code signing procedures.
- Communications security – if the product includes network communications, the network interfaces shall implement strong network security practices such as TLS 1.2+.
- Hardware Interface lockdown – if the product includes any hardware interface that is accessible externally (JTAG, USB, UART, etc) they shall be disabled or encrypted.
- Software Interface lockdown – if the product includes any software port that is open, those ports must either be shut down or appropriately secured.

2.4. Access Control

2.4.1. The product requirements will include a detailed description of all roles (groups, privileges, authorizations) used in the application.

2.4.2. The product requirements will also indicate all the assets and functions provided by the application.

2.4.3. The product requirements will fully specify the exact access rights to each asset and function for each role. An access control matrix is the suggested format for these rules.

2.4.4. Access to, and use of, audit tools that interact with the organizations information systems will be appropriately segmented and restricted to prevent compromise and misuse of log data.

2.4.5. Contractor shall provide the access control list to Resideo Security representatives in accordance with the Resideo's requirements while providing product, software / firmware.

2.5. Error Handling

2.5.1. The product requirements will detail how errors occurring during processing will be handled. Some applications should provide best effort results in the event of an error, whereas others should terminate processing immediately.

2.5.2. The product will implement a philosophy of limited information disclosure in the event of an error. This means error messages will not contain any information regarding the content of the code, filesystem, database schema, etc.

2.6. Logging

2.6.1. The product requirements will specify what events are security-relevant and need to be logged, such as detected attacks, failed login attempts, and attempts to exceed authorization.

2.6.2. The product requirements will also specify what information to log with each event, including time and date, event description, application details, and other information useful in forensic efforts.

2.6.3. Contractor shall provide the event log list to Resideo Security representatives in accordance with the Resideo's requirements while providing product, software / firmware.

2.7. Connections to External Systems

2.7.1. The product requirements will specify how authentication and encryption will be handled for all external systems, such as databases, directories, and web services.

2.7.2. All credentials required for communication with external systems will be stored outside the code in a configuration file in encrypted form.

2.7.3. Contractor shall provide a list of the external and internal interfaces to Resideo Security representatives in accordance with Resideo's requirements while providing product, software / firmware.

2.7.4. All unnecessary internal / external interfaces shall be disabled in the factory.

2.8. Encryption

2.8.1. The product requirements will specify what data must be encrypted, how it is to be encrypted, and how all certificates and other credentials must be handled.

2.8.2. The product will use standard algorithms implemented in a widely used and tested encryption library. Contractor shall not include their own encryption algorithms or their own proprietary implementations of standard algorithms in any products or services supplied to Resideo.

2.8.3. The input factors shall be unpredictable if the symmetric key is derived from the derivation algorithm.

2.8.4. Contractor shall provide the key list to Resideo Security representatives in accordance with the Resideo's requirements while providing product, software / firmware.

2.9. Availability

2.9.1. The product requirements will specify how it will protect against denial of service attacks. All likely attacks on the application should be considered, including authentication lockout, connection exhaustion, and other resource exhaustion attacks.

2.10. Secure Configuration

2.10.1. The product requirements will specify that the default values for all security relevant configuration options will be secure.

2.10.2. For audit purposes, the software should be able to produce an easily readable report showing all the security relevant configuration details.

2.11. Specific Vulnerabilities

2.11.1. The product requirements will include a set of specific vulnerabilities that will not be found in the software.

2.11.2. If not otherwise specified, then the software will not include any of the flaws described in:

- The current "OWASP Top Ten Most Critical Web Application Vulnerabilities."
- The current "Common Weaknesses Enumeration (CWE) top 25."
- The current "Others on the CWE cusp list from top26 to top41."

2.12. Security Manual

2.12.1. The purpose of the Security Manual is to provide the information necessary for those involved in the installation and maintenance of a product or system to understand the requirements for configuring and managing the security of the product or system.

2.12.2. The security manual may be a standalone document, or it may be a chapter in a product manual. This decision lies in the overall size of the security manual.

2.12.3. Below is a list of chapters that should be considered for inclusion in a security manual. For smaller products not all chapters are necessary. For larger systems deployed on commercial operating systems all chapters may be necessary.

- Introduction
- Security Checklists

- Developing a Security Program
- Disaster Recovery Planning
- Physical and Environmental Considerations
- Security Updates and Service Packs
- Virus Protection
- Network Planning and Security
- Virtual Environments
- Securing Wireless Devices
- System Monitoring
- Windows Domains
- Securing Access to the Operating System
- Security Features
- Network Ports Summary
- Glossary

3. Product Cloud Requirements

3.1. All cryptographic keys used in the Cloud Computing shall be distributed and stored securely in an encrypted format.

3.2. Contractor shall use hosted (private and on-premise) password management solution to manage any accounts with full administrative access to manage Information Systems that are used to provide Cloud Computing.

3.3. Contractor shall require multi-factor authentication and network address restrictions be used for any accounts with full or privileged access to manage Information Systems that are used to provide Cloud Computing.

3.4. Contractor shall use isolated network segments for remote management of Information Systems, for virtualization operations (e.g. virtual machine migration) and storage operations (e.g. iSCSI) that are used to provide Cloud Computing.

3.5. Contractor shall ensure that access to any virtualization management functions, administrative consoles, Application Programming Interfaces (APIs) or any other management components must be restricted to Contractor Personnel based upon the principles of least privilege and supported through technical controls (i.e., multi-factor authentication, IP address filtering, encryption in-transit, network segmentation and audit logging).

3.6. Contractor shall ensure that it can identify, preserve, collect, and produce reasonably required electronically stored information on the Cloud Computing in the event of a Security Incident.

3.7. Contractor shall use an Identity and Access Management (IAM) solution to manage authentication, authorization and accounting for any user (human) accounts used to access Information Systems that are used to provide Cloud Computing.

3.8. Contractor shall use secure jump hosts to access Information Systems that are used to provide Cloud Computing and ensure that access to such jump hosts is restricted to Contractor Personnel based upon the principles of least privilege and supported through technical controls.