September 21, 2022

UL Solutions
Supplier Global Cybersecurity Requirements

1. **Purpose**
   1.1. This Supplier Global Cybersecurity Requirements document describes the minimum cybersecurity requirements that Supplier shall comply with in performing services for, or otherwise accessing data belonging to, the contracting entity or entities including their Affiliates (the "UL") under the applicable service agreements, statements of work, or any other related documents (collectively, "Agreements"). All capitalized terms not defined herein shall have the meaning set forth in the Agreements.

2. **Global Cybersecurity Management Program**
   2.1. Supplier shall have an Information Security Management Program ("ISMP") that addresses the overall security program of Supplier. The ISMP shall be formally documented, and such records shall be protected, controlled, and retained according to applicable international, federal, state, or internal requirements.
   2.2. Supplier management support for the ISMP shall be demonstrated through signed acceptance or approval by management.
   2.3. UL shall have the right to assess the effectiveness of the ISMP by reviewing Supplier's information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management support at least annually.

3. **Access Control**
   3.1. **Access Control Policy.** Supplier shall establish, document, and, upon UL's request, communicate to UL, a formal access control policy based on business and security requirements for access. Access control rules shall account for and reflect Supplier's policies for information dissemination and authorization, and these rules shall be supported by formal procedures and clearly defined responsibilities. Access control rules and rights for each user or group of users shall be clearly stated. Access controls must be both logical and physical. Users and service providers shall be given a clear statement of the business requirements to be met by access controls. The policy shall be reviewed and updated at least annually.
   3.2. **Review of User Access Rights.** All access rights shall be regularly reviewed by management through a formal documented process.
      3.2.1. **User Registration**. Supplier shall implement and document a user registration and de-registration procedure for granting and revoking access. User account types shall be identified and conditions for group and role membership shall be established.
      3.2.2. **User Identification and Authentication**. Supplier shall require users to have unique identifiers (user IDs) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of the user. Supplier shall provide a list of all user accounts that will have access to UL Confidential Information on an as needed basis. Authentication and authorization mechanisms shall be applied for users and equipment.
      3.2.3 **User Attestation**. Supplier shall perform, at least bi-annually, an all-user attestation process. The User Attestation process is an ongoing review and confirmation of user access that will

correlate users with their access to systems and applications, evaluate risk associate with required access and deem user access as risky or inappropriate.

3.2.4. **Privilege Management**. Supplier shall restrict and control the allocation and use of privileges to information systems and services through a formal authorization process. Privileges shall be allocated to users on a need-to-use basis and on least privileges in line with the access control policy.

3.3. **Secure Log-on Procedures**. Supplier shall control user access to operating systems with secure log-on procedures that will display general notice warnings that computers may: (i) only be accessed by authorized accounts; (ii) limit the number of unsuccessful log-on attempts; (iii) enforce recording of unsuccessful attempts; (iv) force time delay before further log-on attempts are allowed; (v) reject any further attempts without specific authorization from an administrator; and (vi) not display the password being entered by hiding the password characters and symbols.

3.3.1. **Password Management.** Supplier shall ensure that passwords are controlled through a formal management process. Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of strong passwords.

3.3.2. **User Authentication for External Connections.** Supplier shall develop and implement appropriate authentication methods to control access of remote users to systems containing UL Confidential Information by requiring the use of password or passphrase and at least one (1) of the following: a cryptographic-based technique, biometric techniques, hardware tokens, software tokens, a challenge/response protocol, or certificate agents.

3.4. **Network Services and Connection Control.** Supplier shall specify the networks and network services to which users are authorized to access. Users shall only be provided with access to internal and external network services that they have been specifically authorized to use. The capability to connect to shared networks shall be restricted in line with the access control policy and requirements of the business applications.

3.4.1. **Equipment Identification in Networks.** Supplier shall use automatic equipment identification as a means to authenticate connections from specific locations and equipment to determine whether or not they are permitted to connect to the Supplier's network.

3.4.2. Remote Diagnostic & Configuration Port-Protection. Supplier shall control the physical and logical access to diagnostic and configuration ports. Controls for the access to diagnostic and configuration ports shall include the use of a key lock. Ports, services, and similar applications installed on a computer or network systems, which are not specifically required for business functionality, shall be disabled or removed.

3.4.3. **Segregation in Networks.** Groups of information services, users, and information systems shall be segregated on networks. Supplier shall implement and maintain security gateways which include but are not limited to firewalls and intrusion detection or protection systems which will forward event data and security alerts to a centralized SEIM system for analysis, reporting, and incident response. Supplier shall perform firewall configuration and Access Control List reviews on a regular basis, but not less often than monthly, to ensure appropriate controls and configurations are applied to limit traffic to only what is required for business operations, shall be used between internal network, external networks, and any demilitarized zone (DMZ).

3.4.4. **Network Protection.** Supplier shall implement and maintain firewalls and intrusion detection or protection systems which will forward event data and security alerts to a centralized SEIM system for analysis, reporting, and incident response. Supplier shall perform firewall configuration and Access Control List reviews on a regular basis, but not less often than monthly, to ensure appropriate controls and configurations are applied to limit traffic to only what is required for business operations.

4. **Human Resources Security**

4.1. **Roles & Responsibilities.** Supplier shall define and document the security roles and responsibilities of employees, contractors, and third-party users in accordance with Supplier's information security policy. Supplier shall ensure that workforce members agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to Supplier's assets associated with information systems and services.

4.2. **Terms and Conditions of Employment.** Supplier shall ensure that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to UL's assets associated with information systems and services.

4.2.1. **Screening.** Supplier shall conduct background verification checks on all candidates for employment, contractors, and third-party users in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

4.2.2. **Disciplinary Process.** A formal sanctions process shall be established and implemented for employees who have violated security policies and procedures.

4.2.3. **Removal of Access Rights.** The access rights of all employees, contractors, and third-party users to information and information assets shall be removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment. Changes of employment or other workforce arrangement shall be reflected in removal of all access rights that were not approved for the new employment or workforce arrangement.

4.3. **Information Security Awareness, Education, and Training.** Supplier shall ensure that all employees, contractors, and third-party users receive appropriate awareness training and regular updates in Supplier’s policies and procedures, as relevant to their job function.

5. **Risk Management**

5.1. **Risk Management Program.** Supplier shall create and implement a comprehensive program that manages the risks to information system operations, assets, and UL Confidential Information. The risk management program shall develop means through which the Supplier shall manage and mitigate risks to UL, including physical and environmental hazards.

5.2. **Risk Assessments.** Supplier shall perform risk assessments to identify and quantify information security risks to UL. Supplier shall account for risks from sources including prior incidents experienced, changes in the environment, and any supervisory guidance. Risk assessments are to be performed at least annually, or when major changes occur in the environment, and the results reviewed annually.

6. **Information Security Policy**

6.1. **Information Security Policy.** Supplier shall develop, publish, and implement information security policy documents. The information security policy shall state the purpose and scope of the policy, communicate management's commitment, describe management's and workforce member's roles and responsibilities, and establish Supplier's approach to managing information security. The documents shall be reviewed at planned intervals or if significant changes occur to ensure the policies' adequacy and effectiveness.

7. **Organization of Information Security**

7.1. **Confidentiality Agreements.** Supplier shall ensure that all personnel who access to UL Confidential Information have agreed to confidentiality or non-disclosure restrictions.

7.2. **Independent Review of Information Security.** Supplier shall review at least annually, or when significant changes to the security implementation occur, Supplier's approach to managing information security and its control objectives, controls, policies, processes, and procedures. The review shall include an assessment of Supplier's adherence to its security plan, address the need for changes to the approach to security in light of evolving circumstances, and be carried out by individuals independent of the area under review who have the appropriate skills and experience.

7.3. **Information Security Framework.** Supplier shall follow a leading, industry recognized cyber security framework, e.g., National Institute of Standards and Technology (NIST), or International Organization for Standardization (ISO) 27001. Each year, Supplier shall complete UL's supplier cybersecurity assessment questionnaire. If Supplier fails to satisfy UL's supplier security assessment in UL's sole opinion, UL may terminate any relevant SOW by giving Supplier fifteen (15) days' prior written notice.

7.3.1. **Regulatory Audits and Examinations.** To the extent permitted by law, Supplier shall notify UL if an international, federal or state regulatory agency requests a review, audit, or other examination of the services or records maintained by Supplier on behalf of UL. Supplier shall fully cooperate with UL and any regulator(s) in the event of an audit or review.

7.4. **Identification of Risks Related to Third Parties**. Supplier shall identify the risks to its information and information assets from business processes involving third parties and then implement appropriate security controls. Supplier shall evaluate any information security risks posed by third parties prior to establishing a relationship with such third party. Once a relationship has been established, Supplier shall evaluate the third party's information systems on a scheduled ongoing basis.

7.4.1. **Addressing Security in Third Party Agreements.** Supplier shall ensure that agreements with third parties involving accessing, processing, communicating or managing its information or information assets, or adding products or services to information assets cover all relevant security requirements. Supplier shall identify and mandate information security controls to specifically address third party access to its information assets. Supplier shall maintain written agreements with its third parties that include an acknowledgement that such third parties are responsible for the security of the information.

7.5. **Evidence of Third-Party Risk Management Program.** For Suppliers that maintain or retain data and provide access to any third party, Supplier shall provide evidence of a third-party risk management program. Upon request from UL, Supplier agrees to provide evidence of an assessment of any third parties that have access to UL's data.

8. **Compliance**

8.1. **Identification of Applicable Legislation.** Supplier shall explicitly define, document, and maintain all relevant statutory, regulatory, and contractual requirements for each information system type. The specific controls and individual responsibilities to meet these requirements shall be similarly defined and documented and then communicated to the user community through a documented security training and awareness program.

8.2. **Protection of UL Records.** Supplier shall protect important records from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

8.3. **Regulation of Cryptographic Controls.** Supplier shall use cryptographic controls in compliance with all relevant agreements, laws, and regulations. Supplier shall implement strong cryptographic controls for secure file transfers, data at rest, and email communications, etc. which may contain sensitive data. The compliance with all relevant regulations shall be reviewed at minimum on an annual basis.

8.4. **Information Systems Audit Controls.** Supplier shall develop audit requirements and activities involving checks on operational systems to minimize the risk of disruptions to business processes. An annual audit planning and scoping process shall exist and consider risk, involvement of technical and business staff, other ongoing projects, and business impacts that may impact the effectiveness of the audit.

8.5. **Payment Card Industry Information Security Standard Requirements.** To the extent Supplier receives, accesses, or transmits cardholder data (e.g., credit or debit card data), Supplier acknowledges its responsibility to secure cardholder data and agrees to comply with applicable Payment Card Industry Information Security Standard requirements.

9. **Asset Management**

9.1. **Inventory and Acceptable Use of Assets.** Supplier shall identify and create an inventory of assets and information. All information systems shall be documented and include rules for acceptable use and a method to accurately identify and assign ownership responsibilities to the proper individuals. The rules for acceptable use shall be communicated to all information system users and describe their responsibilities and expected behavior with regard to information and information system usage.

9.2. **Classification Guidelines.** Supplier shall implement and maintain a process to classify information based on its relevant legal requirements, sensitivity, and its criticality to Supplier so that limitations can be put on the data internally and externally. Appropriate procedures for information labeling and handling shall be developed based on the classification system adopted by the Supplier.

9.3. **Information Labeling and Handling.** Supplier shall implement and maintain an appropriate set of procedures for information labeling and handling in accordance with the classification scheme adopted by Supplier. Sensitive information shall be physically and/or electronically labeled and handled appropriately regarding the level of risk the information or document contains.

10. **Physical and Environmental Security**

10.1. **Physical Security Perimeter.** Supplier shall protect areas that contain information and information assets with security perimeters (barriers such as walls, card-controlled entry gates, or manned reception desks). These areas shall not be located in areas that are unattended or have unrestricted access by the public.

10.2. **Physical Entry Controls.** Supplier shall protect secure areas with appropriate entry controls to ensure only authorized personnel are allowed access. Supplier shall maintain visitor access logs for facilities where information systems reside.

10.2.1. **Working in Secure Areas.** Supplier shall design and apply physical protection and guidelines for working in secure areas. The arrangements for working in secure areas shall include controls for the employees, contractors, and third-party users.

10.2.2. **Public Access Areas.** Supplier shall control access points, such as delivery and loading areas, and other points where unauthorized persons may enter the premises and, if possible, isolate them from information processing facilities to avoid unauthorized access.

10.3. **Securing Offices, Rooms, and Facilities.** Supplier shall design and apply physical security for offices, rooms, and facilities to restrict access from the public.

10.4. **Equipment Siting.** Supplier shall site or protect equipment to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.

10.4.1. **Supporting Utilities.** Supplier shall protect equipment from power failures and other disruptions caused by failures in support utilities. Support utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning, shall be regularly inspected and tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.

10.5. **Cabling Security.** Supplier shall protect power and telecommunications cabling carrying data or supporting information services from interception or damage. Clearly identifiable cable and equipment markings shall be used to minimize handling errors and access to patch panels and cable rooms shall be controlled.

10.6. **Equipment Maintenance.** Supplier shall correctly maintain equipment to ensure its continued availability and integrity by developing, communicating, and reviewing / updating a formal, documented information system maintenance policy and procedures.

10.7. **Secure Disposal or Re-Use of Equipment.** Supplier shall check all items of equipment containing storage media to ensure that UL Confidential Information and licensed software has been removed or securely overwritten prior to disposal. Surplus equipment shall be stored securely while not in use. Devices containing UL Confidential Information shall be physically destroyed or the information shall be destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. Certificate of destruction is required to be provided by Supplier upon deletion of UL Confidential Information.

10.8. **Removal of Property.** Supplier shall ensure that equipment, information, or software shall not be taken off site without prior authorization and documentation. Employees, contractors, and third-party users who have authority to permit off-site removal of assets shall be clearly identified.

11. **Communications and Operations Management**

11.1. **Documented Operations Procedures.** Supplier shall formally document and maintain operating procedures and make them available to all users who need them. The documented procedures shall be prepared for system activities associated with information and communication assets.

11.2. **Change Management.** Supplier shall control and archive changes to information assets, systems, networks, and network services. Formal change management responsibilities and procedures shall be in place to ensure satisfactory control of all changes.

11.3. **Segregation of Duties.** Supplier shall enforce the separation of duties to reduce opportunities for unauthorized or unintentional modification or misuse of Supplier's assets. No single user shall be able to access, modify, or use assets without authorization or detection. Supplier shall identify duties that require separation and define information system access authorizations to support separation of duties.

11.4. **Separation of Development, Test, and Operational Environments.** Supplier shall separate and control development, test, and operational environments to reduce the risks of unauthorized access or changes to the operational system.

11.5. **Monitoring and Review of Third-Party Services.** Supplier shall regularly monitor and review the services, reports, and records provided by third parties. Audits shall be carried out regularly to govern and maintain compliance with the service delivery requirements.

11.5.1. **Managing Changes to Third Party Services.** Supplier shall ensure that third parties use appropriate change management procedures for any changes to their provision of services or internal system. Changes to the provision of services, including maintaining and improving existing information security policies, procedures, and controls shall be managed, taking account of the criticality of business systems and processes involved and reassessment of risks.

11.6. **System Acceptance.** Supplier shall establish acceptance criteria for new information systems, upgrades, and new versions. Suitable tests of the systems shall be carried out during development and prior to acceptance to maintain security. Management shall ensure that requirements for acceptance of new systems are clearly defined, agreed upon, and documented.

11.7. **Controls Against Malicious Code.** Supplier shall implement detection, prevention, and recovery controls to protect against malicious code, and also provide appropriate user awareness procedures. Formal policies shall be required, and technologies implemented for the timely installation and upgrade of the protective measures, including the installation and regular, automatic updating of anti-virus or anti-spyware software, including anti-virus definitions, and additional end point security controls should be implemented, such as windows firewall, and Data Loss Prevention solution, etc., and to be current whenever updates are available. Periodic reviews/scans shall be required of installed software and the data content of systems to identify and, where possible, remove any unauthorized software.

11.8. **Back-up.** Supplier shall create and regularly test back-up copies of information and software and store them in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site. A formal definition of the level of back-up required for each system shall be defined and documented including the scope of data being imaged, frequency of imaging, and duration of retention. This document shall be based on the contractual, legal, regulatory, and business requirements.

11.9. **Network Controls**. Supplier shall manage and control networks in order to protect UL from threats and to maintain security for the network, including information in transit. Supplier shall implement controls to ensure the security of information in networks and the protection of connected services from unauthorized access. Controls shall be implemented to ensure the availability of network services and information services using the network. Responsibilities and procedures shall be established for the management of equipment on the network, including equipment in user areas.

11.10. **Management of Removable Media**. Supplier shall document and implement formal procedures for the management of removable media. Media containing UL Confidential Information shall be physically stored and its data encrypted in accordance with the Supplier's data protection and privacy policy on the use of cryptographic controls until the media is destroyed or sanitized, and commensurate with the confidentiality and integrity requirements for its data classification level.

11.10.1. **Physical Media in Transit.** Supplier shall protect media containing UL Confidential Information against unauthorized access, misuse, or corruption during transportation beyond Supplier's physical boundaries.

11.11. **Exchange Agreements.** Supplier shall establish and implement agreements for the exchange of information and software between Supplier and its third parties. The agreements shall specify the minimum set of controls on responsibility, procedures, technical standards, and solutions.

11.12. **Audit Logging.** Supplier shall produce audit logs recording user activities, exceptions, and information security events and keep them for an agreed period to assist in future investigations and access control monitoring. Retention for audit logs shall be specified by Supplier and retained accordingly.

11.13. **Protection of Log Information.** Supplier shall protect logging systems and log information against tampering and unauthorized access. Access to system audit tools and audit trails shall be limited to those with a job-related need.

11.14. **Monitoring System Use.** Supplier shall establish procedures for monitoring use of information processing systems and facilities to check for use and effectiveness of implemented controls. The result of the monitoring activities shall be reviewed periodically. Supplier shall comply with all relevant legal requirements applicable to its monitoring activities. Items that shall be monitored include authorized access and unauthorized access attempts.

11.15. **Clock Synchronization.** Supplier shall ensure that the clocks of all relevant information processing systems within the Supplier's environment have been synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines.

12. **Information Systems Acquisition, Development and Maintenance**

12.1. **Input Data Validation.** Supplier shall apply checks to the input of business transactions, standing data, parameter tables, and information into applications and databases when system development is being performed to ensure that data is correct and appropriate.

12.2. **Output Data Validation.** Supplier shall validate data output from an application to ensure that the processing of stored information is correct and appropriate to the circumstances. Output validation shall be manually or automatically performed when system development on applications and database is being conducted.

12.3. **Policy on the Use of Cryptographic Controls.** Supplier shall develop and implement a policy on the use of cryptographic controls and support it with formal procedures. The cryptographic policy shall be aligned with the Supplier's data protection and privacy policy and shall address the use of encryption for protection of information transported by mobile or removable media, devices, or across communication lines.

12.4. **Key Management.** Supplier shall support the use of cryptographic techniques with the practice of key management. All cryptographic keys shall be protected against modification, loss, and destruction. Secret and private keys shall require protection against unauthorized disclosure, and all cryptographic keys shall be limited to the fewest number of custodians necessary. Equipment used to generate, store, and archive keys shall be physically protected, and encryption keys shall be stored separately from encrypted data.

12.5. **Protection of System Test Data.** Supplier shall carefully select, protect and control test data in non-production environments. The use of operational databases containing UL Confidential Information for non-production purposes shall be avoided. UL Confidential Information must not be used for testing purposes.

12.6. **Access Control to Program Source Code.** Supplier shall restrict access to program source code and associated items to prevent the introduction of unauthorized functionality and avoid unintentional changes.

12.7. **Outsourced Software Development.** Supplier shall supervise and monitor outsourced software development. Supplier shall have a contract for the outsourced development in place with the third party

and address licensing arrangements, certification of the quality and accuracy of the work carried out, rights of access for audit of the quality and security functionality of code.

12.8. **Control of Technical Vulnerabilities and Penetration Testing.** Supplier shall perform vulnerability scans at intervals consistent to industry best practices to identify potential technical vulnerabilities based on notification of ZERO-day vulnerabilities. Supplier shall subscribe to industry recognized threat monitoring service. Once a potential technical vulnerability has been identified, Supplier shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls. Supplier shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required. Supplier shall agree in writing that prior to production the application will undergo a vulnerability and source code analysis. Postproduction, Supplier shall perform contractually agreed upon security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase. Supplier shall provide written documentation to UL of the results of the scans and tests along with a mitigation plan. Supplier shall agree in writing that these vulnerabilities shall be mitigated pursuant the policies of each Customer entity.

13. **Information Security Incident Management**

13.1. **Reporting Information Security Incidents.** Supplier shall report Security Incidents through appropriate communications channels in accordance with the Agreements. All employees, contractors, and third-party users shall be made aware of their responsibility to report any Security Incidents as quickly as possible. Formal Security Incidents reporting procedures to support Supplier's corporate policy shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of a Security Incident, treating the breach as discovered, and the timelines of reporting and response. Supplier standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.

13.2. **Responsibilities and Procedures.** Supplier shall establish management responsibilities and procedures to ensure a quick, effective, and orderly response to Security Incidents.

13.3. **Incident Response Plan.** Supplier shall be able to implement and maintain an existing incident response plan containing milestones and service level-agreements for its incident response capability, describing the structure and organization of the incident response capability, providing a high-level approach for how the incident response capability aligns with its overall organizational policies and procedures, and meets the unique requirements of the Supplier, which relate to mission, size, structure, and functions. The incident response plan will also define reportable incidents and resources needed to effectively maintain and mature an incident response capability, as well as provide metrics for measuring the incident response capability. The plan shall then be approved by designated Supplier officials.

13.3.1. Copies of the incident response plan shall be distributed to incident response personnel and Supplier organization elements.

13.3.2. Reviews of the incident response plan shall occur annually and include a table-top exercise, documentation, test plan, and results.

13.3.3. Revisions to the incident response plan shall be made to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

13.3.4. Supplier shall communicate incident response plan changes to incident response personnel and organizational elements.

13.4. **Collection of Evidence.** Supplier shall collect, retain, and present evidence after a Security Incident. The evidence that is collected, retained, and presented shall be done in accordance with the laws of the relevant jurisdiction(s).

14. **Disaster Recovery Plan and Business Continuity Management**

14.1. **Including Information Security in the Disaster Recovery Plan and Business Continuity Management Process.** Supplier shall develop and maintain a managed program and process to maintain or restore operations and ensure availability of information, at the required level and in the required time frames following interruption to, or failure of, critical business processes for business continuity. Supplier shall maintain a single framework of business continuity plans to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. The program and process shall identify all the assets involved in critical business practices, consider the purchase of suitable insurance, ensure the safety of personnel and the protection of information assets, formulate and document business continuity plans, and address information security requirements in line with the agreed upon business continuity strategy. Supplier must provide results of Business Continuity Planning (BCP) sessions on an at least annual basis. BCP exercises must be conducted and reviewed with all downstream suppliers. Supplier will document BCP processes and procedures in support of products and services provided. This includes plans for the loss of critical resources including workplace, work force, third-party suppliers, and applications.

14.2. **Testing, Maintaining, and Re-Assessing Business Continuity Plans.** Supplier shall test and annually update business continuity plans to ensure that they are up to date and effective. The business continuity plan tests shall ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.