Service Provider Information Security Controls

Table of Contents

1. Definitions and Interpretations

1.1 The following terms used have the following meanings:

Anonymised	means data from which all personal data has been removed, so that it is no longer possible to re-identify an individual from the information; taking into account all means reasonably likely to be used by the Service Provider or anyone else to re-identify an individual.
Demilitarized Zone	means a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network (e.g. the Internet). An external network node can only access what is exposed in the DMZ, while the rest of the network is firewalled.
Personal Data	means any information, including information in electronic form, relating to a living person who can be identified (a) from those data or (b) from those data and the use of additional information, taking into account all means reasonably likely to be used by anyone to identify the person directly or indirectly; and includes, without limitation, first and last names, ID numbers, including government-issued identifiers, personal dates such as birthdates, email addresses, location data, internet protocol address or other online identifiers and information concerning race, ethnicity or mental or physical health. For clarity, personal data includes personal data that is publicly available and excludes personal data that has been anonymised so that it is no longer possible to re-identify an individual from the information; taking into account all means likely reasonably to be used by the Service Provider or anyone else to re-identify an individual.
Privileged User	means a user who has been allocated powers within the computer system which are significantly greater than those available to the majority of users.
Processing	means any operation or set of operations performed upon PwC member firm information, including personal data, whether or not by automatic means. This includes operations such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.
Risk Assessment	means a planned activity undertaken to identify information security risks, evaluate their potential impact and likelihood, including their impact on individuals who are the subject of any personal data, and compare to established risk criteria for acceptance or remediation.
Risk Treatment	means actions taken to address identified information security risks, such as implementing or enhancing controls to remediate risks or accepting risks based on risk criteria.
Sanitised	means when data in a development or test environment is disguised by overwriting it with realistic looking, but false, data of a similar type (e.g. by masking or substitution techniques, etc.)

2. Risk Assessment and Treatment

2.1 Service Provider shall perform a Risk Assessment periodically and upon significant organizational, information technology, or other relevant changes. Service Provider shall document the risk assessment results and implement corresponding risk treatment plans.

3. Management Direction for Information Security

Information Security Policy

3.1 Service Provider shall implement a written information security policy that is (a) comprehensive, addressing the information security risks and controls identified through the Risk Assessment process, for each area of information security (i.e., user access, system development and change, business continuity, etc.) (and supplemental policies should be developed and implemented as appropriate); (b) reflects the requirements of applicable law, including Data Protection laws; (c) approved by management; (d) published and communicated to all employees and applicable third-party contractors; and (e) annually reviewed and updated to address (i) relevant organizational changes, (ii) contractual requirements owed to PwC, (iii) identified threats or risks to information assets, and (iv) relevant changes in applicable laws and regulations.

Information Security Management Program

3.2 Service Provider shall have a specific function, composed of suitably qualified information security specialists, to lead the information security management program. The specific function shall be ratified and supported by Service Provider's business leadership. Responsibilities shall include (a) developing and maintaining the security policy and any supplemental requirements; and (b) identifying accountability for the execution of information security activities.

Personnel Confidentiality Obligations

3.3 Service Provider management shall require employees and third-party contractors with access to PwC Data to commit to written information security, confidentiality, and privacy responsibilities with respect to that information. These responsibilities must be binding and shall survive termination or change of employment or engagement. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of PwC Data.

4. Human Resource Security

Background Screening

4.1 Service Provider shall perform background verification checks on employees or third-party contractors that have access to PwC Data, including personal data, in accordance with relevant laws, regulations, and ethical requirements for each individual at least upon initial hire (unless prohibited by law). The level of verification shall be appropriate according to the role of the employee or third-party contractor, the sensitivity of the information to be accessed in the course of that person's role, and the risks that may arise from misuse of the information. The following checks shall be performed for each individual at least upon initial hire, unless prohibited by law: (i) identity verification, (ii) criminal history, (iii) employment history, and (iv) education verification.

Information Security Training

4.2 Service Provider shall provide information security awareness training to employees and applicable third-party contractors upon hire and at least annually thereafter. Such training shall (a) be updated to include changes in organizational policies and procedures; (b) be relevant to trainee job functions; (c) communicate the formal disciplinary process in effect when Personnel commit an information security breach; (d) include specific data protection training for personal data; and (e) include phishing awareness, either by simulations or explicitly in an annual course.

5. Access Control

User Access Management

5.1.1 Service Provider shall implement formal, documented access control policies to support creation, amendment, and deletion of user accounts for systems or applications holding or allowing access to PwC Data. Service Provider shall implement a formal, documented user account and access provisioning process to assign and revoke access rights to systems and applications. User account privileges shall be allocated on a "least privilege" basis and shall be formally authorized and documented. Service Provider shall prohibit the use of "generic" or "shared" accounts without system controls enabled to track specific user access and prevent shared passwords.

5.1.2 Privileged user access rights shall be (a) restricted to users with clear business need; (b) assigned to a separate user account, to be used only for the time period required to complete the necessary task; (c) segregated appropriately (e.g., code migration, security administration, audit log permissions, production support administration, etc.); (d) captured by system logs and periodically reviewed; and (e) accomplished by multi-factor authentication.

5.1.3 Service Provider shall monitor and restrict access to utilities capable of overriding system or application security controls. Administrator access rights to workstation endpoints shall be restricted. System and application owners shall review user access rights for appropriateness, at least on a quarterly basis. Inappropriate access shall be revoked immediately upon identification.

5.1.4 Accounts on systems and applications storing or enabling access to PwC Data shall be disabled upon 90 days of inactivity. Access modification confirmation shall be communicated to system owners when complete. User access rights to systems and applications storing or allowing access to PwC Data shall be removed upon termination or change of employment responsibilities. Specifically, user access rights shall be (a) removed within 24 hours, upon termination of employment and (b) reviewed and adjusted within one week, upon change of employment responsibilities.

5.1.5 User access to systems and applications storing or allowing access to PwC Data shall be controlled by a secure logon procedure. To support this, Service Provider shall implement the following controls for user authentication: (a) each user account ID shall be unique; (b) each user account shall have a password; (c) passwords shall be echo-suppressed on screen or masked on print-outs; (d) if set by system administrator, initial password issued shall be random and shall be changed by the user upon first use; (e) users should set their own passwords as part of a password management system; (f) passwords shall be treated as confidential data and shall be encrypted upon transmission; (g) implement a password policy that (i) restricts reuse of passwords for at least ten (10) previous versions; (ii) enforces password changes at least every ninety (90) days; (iii) enforces account lock-out after five (5) failed login attempts; (iv) requires password complexity (passwords shall be a minimum of eight (8) alphanumeric characters (20 characters for privileged accounts) and shall include a mix of upper- and lowercase characters with at least one (1) numeric and one (1) special character; (h) passwords shall be stored using a one-way encryption mechanism; and (j) service account passwords shall be at least thirty (30) characters in length and shall be configured to prevent interactive logon. Where a password of at least 30 characters is not possible, passwords shall be set to the maximum length allowed by the system and shall be changed every 90 days through a password management system or procedure. For PwC end users, Service Provider shall support either integration with PwC-approved authentication mechanisms (e.g. federation) or multi-factor authentication.

6. Physical Access Management

6.1 Physical access to facilities where PwC Data is stored or processed shall be restricted to authorized Personnel. Controls shall include all of the following, unless prohibited by law: (a) strong locks enabled by key pads or swipe card technology; (b) locked windows and doors for vacant facilities and for facilities during non-operating hours; (c) installed, remotely-monitored alarm systems, monitored CCTV, and/or on-premise security guards at all times; (d) where legally permissible, photographic access credentials worn visibly, clearly designating employee, third-party contractor, or visitor; (e) visitor escort at all times while in areas where PwC Data is stored or processed; and (f) documented quarterly review of physical access logs and access control lists. Sensitive physical locations should be isolated from the rest of the facility where possible.

7. Protection of Equipment

7.1 Equipment storing or processing PwC Data shall be located within a dedicated, secured, and isolated facility (e.g., data centre, server room). Power and telecommunications cabling carrying data or supporting information services shall be protected from interruption, interference, or damage. Information processing equipment and storage media containing PwC Data shall be protected during

physical transport. In particular, Service Provider shall (a) use authorized couriers; (b) maintain adequate insurance; and (c) use appropriate secure packaging, based on the relevant data classification.

7.2 Users shall protect unattended sessions and equipment. System and application sessions shall automatically terminate or revalidate after a maximum of (a) 15 minutes for systems and applications handling Confidential or Highly Confidential PwC Data, or (b) 60 minutes of inactivity for all other systems and applications. Additionally, a clear desk and clear screen policy shall be enforced.

7.3 Printers shall require authentication controls to reduce the opportunity for unauthorized access to PwC Data. Service Provider shall implement controls to protect equipment, information, and assets located off-premise and/or during remote access sessions such as teleworking or remote administration. Teleworking, mobile device, and removable media policies shall be implemented and enforced. Service Provider shall encrypt remote access communications to systems or applications containing PwC Data and shall require a minimum of multi-factor authentication, Virtual Private Networking (VPN) device access or equivalent, and restricted ports and protocols.

7.4 Personally, owned and managed equipment shall not be used to access or store PwC Data. A BYOD model shall be controlled by Service Provider and contain controls commensurate with those on corporate-owned devices. Removable media devices (e.g. USB drives, memory sticks, Bluetooth storage devices) storing PwC Data shall be read-only and data shall be encrypted. Mobile devices (e.g. smartphones, tablets) shall not be used as removable media. Temporary write access shall be authorized through a formal risk review process and shall enforce encryption. Metadata logs shall be generated and stored separately from the removable media.

7.5 Service Provider shall implement procedures to ensure that PwC Data, including personal data, is securely destroyed when no longer needed for the purposes authorized by PwC or at the expiration or termination of the Agreement. In particular: (a) secure erasure of PwC Data shall be confirmed prior to asset destruction and disposal; (b) Service Provider shall maintain records of destruction; and (c) Service Provider shall require any third parties engaged to process PwC Data to securely dispose of the information when no longer needed for the services they are required to deliver.

8. Environmental Control

General

8.1 Service Provider shall implement environmental controls to protect Personnel and equipment used to process or store PwC Data, including personal data. These controls shall include all of the following, unless prohibited by law: (a) fire suppression systems shall be installed, actively maintained, and periodically tested; (b) temperature and humidity controls shall be installed within a data centre or server room environment; (c) arrangements shall maintained with authorities for active response to civil unrest or natural disasters; and (d). backup power technology (e.g., uninterruptible power supply, diesel generator, separate grid connection) shall be installed, actively maintained, and periodically tested.

Environmental Risk Assessment

8.2 Service Provider shall implement environmental controls to protect Personnel and equipment used to process or store PwC Data, including personal data. These controls shall include all of the following, unless prohibited by law: (a) fire suppression systems shall be installed, actively maintained, and periodically tested; (b) temperature and humidity controls shall be installed within a data centre or server room environment; (c) arrangements shall maintained with authorities for active response to civil unrest or natural disasters; and (d). backup power technology (e.g., uninterruptible power supply, diesel generator, separate grid connection) shall be installed, actively maintained, and periodically tested.

9. Asset Management

Asset Register

9.1 Assets that store or process PwC Data shall be identified and included within an asset register. At a minimum, version, license, and ownership information, shall be included for each asset within the register. Information assets shall be classified according to asset value, criticality, sensitivity, and the risks resulting from unauthorized disclosure of the information. Procedures for labelling and handling information assets shall be developed for each asset classification.

Use of Assets

9.2 Employees and third-party contractors shall agree to documented policies for the acceptable use and handling of assets. Assets shall be returned immediately upon termination of employment, and return of assets shall be tracked and verified.

System Hardening

9.3 Service Provider shall implement formal, documented system hardening procedures and baseline configurations. Unsupported software or hardware shall not be used.

10. Communications Security

Network Security

10.1 Service Provider shall segregate network systems containing PwC Data from network systems supporting internal or other activity. Service Provider shall logically segregate PwC Data within a shared service environment. Service Provider shall secure network segments from external entry points where PwC Data is accessible.

10.2 External network perimeters shall be hardened and configured to prevent unauthorized traffic. External connections shall terminate in a Demilitarized Zone (DMZ) and connections shall be recorded in event logs. Inbound and outbound points shall be protected by firewalls and intrusion detection systems (IDS). Communications shall be limited to systems strictly allowed, and if possible, intrusion prevention systems (IPS) shall be used. Ports and protocols shall be limited to those with specific business purpose. Web and application servers shall be separated from corresponding database servers by the use of firewalls.

10.3 Service Provider shall implement access controls on wireless networks commensurate with the security level of external virtual private network (VPN) access points. Strong encryption and strong authentication (e.g., WPA2) shall be used.

10.4 Service Provider shall implement access controls on wireless networks commensurate with the security level of external virtual private network (VPN) access points. Strong encryption and strong authentication (e.g., WPA2) shall be used.

10.5 Service Provider shall implement Internet filtering procedures to protect end user workstations from malicious websites and unauthorized file transfers outside the network. Only authorised file sharing websites and tools shall be used for business purposes. Access to unauthorised file sharing websites and tools shall be blocked.

11. Cryptographic Controls

Encryption

11.1 PwC Data, including personal data, shall be encrypted at rest.

Key Management

11.2 Service Provider shall implement cryptographic key management procedures that include the following: (a) generation of cryptographic keys with approved key lengths; (b) secure distribution, activation and storage, recovery, and replacement/update of cryptographic keys; (c) immediate

revocation (deactivation) of cryptographic keys upon compromise or change in user employment responsibility; (d) recovery of cryptographic keys that are lost, corrupted or have expired; (e) backup and archive of cryptographic keys and maintenance of cryptographic key history; (f) allocation of defined cryptographic key activation and deactivation dates; (g) restriction of cryptographic key access to authorized individuals; and (h) Complying with local legal and regulatory requirements.

12. Information Exchange and Transfer

12.1 PwC Data, including personal data, shall be encrypted during transmission across networks, including over untrusted networks (e.g., public networks) and when writing to removable devices. Service Provider shall use platform and data-appropriate encryption (e.g., AES-256) in non-deprecated, open/validated formats and standard algorithms. Certificates used for encryption in transit shall be obtained from an acknowledged certification authority.

13. Cloud Controls

13.1 Service Provider shall encrypt data during transmission between the Internet, the cloud environment, and the PwC network; between each application tier; and between interfacing applications. Cryptographic keys shall be supplied and governed by the PwC Member Firm (e.g., creation, rotation, and revocation). Management and usage of cryptographic keys shall be segregated duties. Where technically feasible, Service Provider shall integrate with PwC's Cloud Access Security Broker (CASB).

14. Operations Security

Service Management

14.1 Service Provider shall define capacity requirements and monitor service availability.

15. Penetration Testing

15.1 Service Provider shall perform annual penetration testing for systems and applications that store or allow access to PwC Data, including personal data, or when significant changes are made to those systems and applications. Upon request by PwC, Service Provider shall provide complete testing results, which shall include the scope and methodology utilized; the number of critical, high, and medium severity findings; the name of the third-party tester; and the date of such third-party testing. Any vulnerability identified during the testing which is defined by PwC as "critical" or "high" risk shall be remediated within ten (10) business days. All other vulnerabilities that do not fall within these categories shall be remediated within 30 days.

16. Vulnerability Management

16.1 Service Provider shall implement a patch and vulnerability management process to identify, report, and remediate system and application vulnerabilities by (a) performing vulnerability scans on a monthly basis and during any major system or application updates; (b) implementing vendor patches or fixes; and (c) developing procedures to address the remediation of identified vulnerabilities. The procedures shall be approved by the application or system owner and by implemented commensurate with the level of risk. From the date that a patch or vendor-approved workaround becomes available, vulnerabilities shall be addressed as follows, and any deviation from this timeframe for "emergency", "critical", and "high" risk vulnerabilities requires PwC's approval: (i) "emergency" within four (4) business days; (ii) "critical" and "high" within ten (10) business days; and (iii) "medium" and "low" within 30 days.

17. Malware Protection

17.1 Service Provider shall implement controls to detect and prevent malware, malicious code, and unauthorized execution of code. Controls shall be updated regularly with the latest technology available (e.g., deploying the latest signatures and definitions).

18. Logging and Monitoring

18.1 Service Provider shall generate administrator and event logs for systems and applications that store, allow access to, or process PwC Data. Logs shall be archived for a minimum of 180 days. Logs shall capture date, time, user ID, device accessed, and port used. Logs shall capture key security event types (e.g., critical files accessed, user accounts generated, multiple failed login attempts, events related to systems that have an Internet connection). Access to modify system logs shall be restricted. Logs shall be provided to PwC upon request. Service Provider shall review system logs periodically (at minimum every 90 days) to identify system failures, faults, or potential security incidents affecting PwC Data. Corrective actions shall be taken to resolve or address issues within any required timeframes.

19. System Development, Acquisition, and Maintenance

19.1 The hardware, software, and service procurement process shall be documented and include identification and evaluation of information security risks.

19.2 Service Provider shall implement formal, documented change control procedures to manage changes to information systems, supporting infrastructure, and facilities. Major changes impacting PwC Data or supporting systems shall be communicated to PwC 30 days prior to implementation. Acceptance criteria shall be established for production change approval and implementation. Stakeholder approval shall be provided prior to change implementation.

19.3 Service Provider shall logically or physically separate environments for development, testing, and production. User access to environments and PwC Data, including personal data, shall be restricted and segregated, based on job responsibilities. User access to program source code shall be restricted and tracked.

19.4 Secure system engineering and coding practices shall be established, documented, and integrated within the system development life cycle (SDLC). Developers shall attend secure development training periodically.

19.5 System and application changes shall undergo testing and meet defined acceptance criteria prior to implementation. Testing shall include relevant security controls.

19.6 PwC Member Firm production data shall not be used within a test environment. If usage is unavoidable, data shall be masked (e.g. obfuscated, sanitised, de-identified, anonymised) or the non-production environment shall have security controls equivalent to those within the production environment.

19.7 Source code shall undergo automated static source code analysis and vulnerability remediation prior to the initial transfer of any PwC Data into Service Provider's environment (unless otherwise agreed by PwC) and after every major release of the source code. Upon PwC's request, Service Provider shall provide PwC with a detailed summary of the analysis, including the scope of the review, raw data results, and any identified vulnerabilities. . Post-implementation testing shall occur subsequent to system changes, to validate that existing applications and security controls were not compromised.

19.8 Service Provider shall monitor outsourced system development activities, subject to third party Service Provider management controls.

20. Third Party Service Provider Management

20.1 Service Provider agreements with third parties processing PwC Data shall include appropriate information security, confidentiality, and data protection requirements, as detailed in the Agreement. Agreements with such parties shall be reviewed periodically to validate that information security and data protection requirements remain appropriate. Service Provider shall review its third parties' information security controls periodically and validate that these controls remain appropriate according to the risks represented by the third party's handling of PwC Data, taking into account any state-of-the-art technology and the costs of implementation.

20.2 Service Provider shall restrict third party access to PwC Data, including personal data. When access to PwC Data is necessary for performance of the contracted service, Service Provider shall (a) provide the PwC Member Firm a list of third parties with required access to PwC Data, including personal data; (b) permit access to PwC Data, including personal data, only as necessary to perform the Services that the third party has contractually agreed to deliver; and (c) record third party access to PwC Data, including personal data, within system logs, subject to Service Provider controls for logging and monitoring.

21. Incident Management

Incident Management Policy

21.1 Service Provider shall implement a formally documented incident management policy that includes: (a) clearly defined management and user roles and responsibilities; (b) reporting mechanism for suspected vulnerabilities and events affecting the security of PwC Data, including personal data (including reporting of suspected unauthorized or unlawful access, disclosure, loss, alteration, and destruction of PwC Data); (c) procedures for assessment of, classification of, and response to, security incidents (response procedures shall be implemented within a reasonable timeframe and proportionate to the nature of the security incident and the harm, or potential harm, caused); (d) procedures for notification to relevant authorities as required by law and the PwC Member Firm, within the timeframes specified in the Agreement; (e) procedures for forensic investigation of a security incident; and (f) a process for incident and resolution analysis designed to prevent the same, or similar, incidents from happening again.

Incident Tracking System

21.2 Service Provider shall maintain a security incident tracking system that documents the following items for each security incident affecting PwC Data: (a) incident type, including how and where the incident occurred; (b) whether there has been any unauthorized or unlawful access, disclosure, loss, alteration or destruction of PwC Data, including personal data; (c) the PwC Data affected by the incident, including the categories of any personal data affected; (d) the time when the incident occurred, or is estimated to have occurred; and (e) remediation actions taken to prevent the same, or similar, incidents from happening again. Incident documentation shall be reviewed quarterly to validate response and resolution.

Investigations

21.3 Service Provider shall support any investigation (e.g., by the PwC Member Firm, law enforcement, or regulatory authorities) that involves PwC Data. Forensic procedures shall be developed to support incident investigation. Engagement with a forensic specialist should be considered. Integrity of event and system log data shall be forensically maintained. Local legal requirements shall be followed.

22. Resilience

Business Continuity, Disaster Recovery

22.1 Service Provider shall perform business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood, and required controls and procedures. Based on risk assessment results, Service Provider shall document, implement, annually test and review business continuity and disaster recovery (BC/DR) plans to validate the ability to restore availability and access to PwC Data in a timely manner in the event of a physical or technical incident that results in loss or corruption of PwC Data. BC/DR plans shall include: (a) availability requirements for PwC Member Firm services,

specifying critical systems and agreed upon recovery points (RPO) and recovery time objectives (RTO); (b) clearly defined roles and responsibilities; (c) provisions for a geographically separate alternate site subject to physical and environmental controls; and (d) backup and restoration procedures that include sanitation, disposal, or destruction of data stored at the alternate site.

Backup Procedures and Media

22.2 Service Provider shall follow industry best practices to make regular, encrypted backups of database and repository files on a timeframe mutually agreed by the parties to a secured location separate from the primary data centre. Service Provider must restore any corrupted files using the most current backup available. Without prior notice to Service Provider, PwC may access the backup records and to review any record of system activity related to PwC. Information backup procedures and media shall include (a) strong encryption technology; (b) integrity validation; (c) reconciliation with disaster recovery requirements; and (d) secure offsite storage supporting availability requirements.

23. Audit and Compliance

Compliance

23.1 Service Provider shall periodically review whether its systems and equipment storing, enabling access to, or otherwise processing PwC Data, including personal data, comply with legal and regulatory requirements and contractual obligations owed to PwC. Service Provider management shall review the technical and organisational controls implemented to protect PwC Data for compliance with agreed-upon information security controls at least annually and report results to senior management.

PwC's Assessment

23.2 Service Provider shall allow PwC to monitor and assess adherence to contractual requirements, including information security controls.

23.2.1 **Remote Assessment.** Service Provider shall promptly review and complete any questionnaire identified by PwC that is provided in an online vendor management assessment tool (e.g., KY3P or similar tool). Service Provider shall make relevant documentation, reports, and/or evidence available for review upon PwC's request.

23.2.2 **Onsite Assessment.** PwC (or its designee) may conduct an independent assessment of Service Provider during normal business hours to verify compliance with this Agreement (i) once per year upon reasonable advance notice, (ii) after a suspected or actual Data Breach, and (iii) if PwC undergoes an audit by a government agency. Such assessment includes (a) inspecting Service Provider's processing facilities and equipment, (b) conducting face-to-face interviews with Service Provider Personnel, (c) running assessment software to test processing applications, and (d) auditing any information technology system involved in the Services. Before commencing any on-site assessment, the parties will agree on the scope, timing, and duration of the assessment. In addition, upon written request of PwC, Service Provider shall produce documentation to prove performance of the applicable security controls.

Audit Reports

23.3 Service Provider shall maintain current independent verification of the effectiveness of its technical and organizational security measures. At least annually, Service Provider shall cause an independent third party to conduct an audit and produce a SOC 2 Type 2 report. Service Provider shall make available to PwC the current SOC 2 Report, including the status of any exceptions identified within the report. Service Provider shall also comply with the controls in, and maintain, a current, valid ISO 27001 Certification. Service Provider shall provide to PwC such certification and a copy of Service Provider's Statement of Applicability (SOA).

Remediation

23.4 Promptly following the completion of each of the audits, assessments, reports, or tests described in Sections 22.1 through 22.3, Service Provider shall prioritize remediation efforts according to the severity

of the vulnerabilities identified during any such audit, assessment, report, or test, and take prompt action to address all identified "critical" or "high" vulnerabilities. Service Provider will remediate or mitigate such "critical" or "high" vulnerabilities within ten (10) days of identification. Service Provider will correct all other identified vulnerabilities within thirty (30) days of discovery. PwC may track and request updates on the timing for completion of Service Provider's remediation efforts. If Service Provider fails to remedy any "critical" or "high" vulnerability as required, then PwC may terminate this Agreement (or the applicable Order) upon notice to Service Provider, without having any obligation or liability to Service Provider.

Disclosure

23.5 PwC may share the results of any audit, report, or test under Sections 22.1 through 22.3 with (i) any PwC Member Firm and (ii) under the protection of appropriate confidentiality measures, actual or prospective clients of any PwC Member Firm. Without the need for confidentiality measures, PwC may share the results of any such audit, report, or test under Sections 22.1 through 22.3 with any government regulator of any PwC Member Firm or any client of any PwC Member Firm. In addition, and to the extent required, Service Provider shall cooperate in good faith with requests from any client or government regulator of any PwC Member Firm that wishes to further investigate Service Provider's security audit attestations and results.

24. Services Termination

24.1 Service Provider shall comply with a documented termination or conclusion of service process. Non-disclosure and confidentiality responsibilities with respect to PwC Data, including personal data, shall remain in place following Agreement termination or conclusion. A primary point of contact shall be identified to support the service termination process. Service Provider shall communicate agreement termination or conclusion to relevant employees and stakeholders. Service Provider shall revoke access to systems and applications storing, allowing access to, or processing PwC Data promptly upon completion or termination of the Agreement. Service Provider shall return hardware, software, middleware, documents, data, information, and other assets owned or leased from the PwC Member Firm. Service Provider shall issue certificates confirming the return and/or destruction of all copies of PwC Data, including personal data, in Service Provider's possession or control, including any information stored on backup media to the PwC Member Firm. Service Provider shall obtain certification of destruction of PwC Data from third-party contractors.