PwC Middle East

Service Provider Information Security Controls

Security Controls

Section 1—Risk Assessment and Treatment

1.1 **Definitions**.

"**Applicable Law**" means all applicable foreign and domestic laws, statutes, ordinances, rules, directives, regulations, orders, or other legally binding instrument, including all applicable Data Protection Laws, anti-money laundering laws, anti-bribery laws, and laws and regulations pertaining to non-discrimination, affirmative action, labor, wages, hours, and other conditions of employment.

"**Data Breach**" means any misuse, compromise, or accidental or unauthorized destruction, loss, alteration, acquisition, disclosure of, or access to PwC Data (including any PwC Data processed by a Subprocessor).

"**Personnel**" means partners, principals, directors, officers, employees, members, representatives, independent contractors and consultants, outsourcers, subcontractors, and agents of either party and its affiliates.

"Privileged User" means a user who has been allocated authority within the computer system that are significantly superior to those available to most users.

"PwC Data" means, collectively, all data, content, documents, software, text, images, audio, video, photographs, or any other information or material in any format

(a) submitted to the Services by users, including

(i) business information of PwC Member Firms and their clients;

(ii) personal data originating with PwC Member Firms or their clients;

(b) created or generated through the Services;

(c) derived or compiled from the data described in **subsections (a)** and **(b)**;

(d) consisting of summaries or analyses involving the data described in **subsections (a)** through **(c)**; and

(e) consisting of PwC Usage Data.

"**PwC Member Firm**" or "**PwC Network Firm**" means the following entities: (a) an entity or firm that is a party to (i) a written agreement with PricewaterhouseCoopers International Limited ("**PwCIL**") for the purpose of participation in PwCIL, or (ii) a Name License Agreement with the PwC Business Trust; (b) an entity or firm that has executed an agreement with any entity described in clause (a) above for the purpose of participating in PwCIL; and (c) a subsidiary or affiliate of an entity or firm in **subsections (a)** or **(b)** above.

"**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.

1.2 **General**. Service Provider shall perform and document Risk Assessments periodically and upon significant organizational or information technology changes. Service Provider shall promptly implement corresponding Risk Treatments.

Section 2—Management Direction for Information Security

2.1 **Information Security Policy**. Service Provider shall publish and implement a management-approved and comprehensive written information security policy that

(a) addresses the information security risks and controls identified through Risk Assessments 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;

(c) applies to all Personnel; and

(d) undergoes annual reviews and is updated to address (i) relevant organizational changes, (ii) PwC contractual requirements, (iii) identified threats or risks to information assets, and (iv) relevant changes in Applicable Law.

2.2 **Information Security Management Program**. Service Provider shall implement a business-approved information security management program that

(a) is composed of qualified information security specialists;

(b) develops and maintains the written information security policy and any supplemental requirements; and

(c) identifies Personnel responsible for the execution of information security activities.

2.3 **Personnel Confidentiality Obligations**. Service Provider shall require Personnel with access to PwC Data to adhere to a binding, management-approved written information security policy designed to preserve and protect the confidentiality and privacy of PwC Data. These obligations survive termination or change of Personnel's employment or engagement. Service Provider shall separate Personnel with conflicting duties and areas of responsibility to protect against unauthorized or unintentional modifications or misuse of PwC Data.

Section 3—Human Resource Security

3.1 **Background Screening**. Unless prohibited by Applicable Law, Service Provider shall perform background verification checks on Personnel that have access to PwC Data upon hire or initiation of engagement. Service Provider shall consider the following when performing background verification checks: (a) the role of the individual; (b) the sensitivity of the PwC Data to be accessed during that individual's role; and (c) the risks that may arise from misuse of the PwC Data.

3.2 **Information Security Training**. Service Provider shall train Personnel on information security awareness upon hire or initiation of engagement and annually thereafter.

Section 4—User Access Management

4.1 **Documentation**. Service Provider shall publish and document (a) access control policies to support the creation, amendment, and deletion of user accounts for systems or applications processing PwC Data; (b) user account and access provision processes to assign and revoke access rights to systems and applications processing PwC Data; and (c) Privileged User account policies allocated on the level of privilege necessary to perform the different functions of the Service. Service Provider shall require that the use of "generic" or "shared" accounts contain system controls enabled to track specific user access and prevent shared passwords.

4.2 **Privileged User Accounts**. With respect to Privileged User accounts, Service Provider shall (a) restrict access to Personnel with clear business needs; (b) provision accounts solely for the duration needed to complete the necessary task; (c) appropriately segregate (e.g., code migration, security administration, audit log permissions, production support administration, etc.); (d) capture and periodically review system logs; and (e) enable access using multi-factor authentication.

4.3 **Access Rights**. Service Provider shall monitor and restrict access to utilities capable of overriding systems or application security controls and shall restrict administrator access rights to workstation endpoints. Application owners shall periodically review user access rights for appropriateness and shall immediately revoke inappropriate or unauthorized access upon detection.

4.4 **Disabling Accounts**. Service Provider shall disable accounts on systems and applications processing PwC Data after a Service Provider-mandated period of inactivity and shall communicate that disabling to system owners when complete. Service Provider shall promptly remove Personnel's user access rights to systems and applications processing PwC Data upon termination of employment or termination of engagement and upon change of employment or engagement.

4.5 **Logon Procedure**.

(a) Service Provider shall implement a secure login procedure for user access and service account access to systems and applications processing PwC Data. To support this, Service Provider shall implement an industry-standard secure login procedure that includes (i) minimum password length, (ii) password complexity, (iii) unique accounts, (iv) random initial passwords, (v) password history, and (iv) password protection at rest and in transit.

(b) For PwC end user authentication, Service Provider shall support either integration with PwC-approved authentication mechanisms (e.g., federation) or multi-factor authentication.

Section 5—Physical Access Management

5.1 **General**. Unless prohibited by Applicable Law, Service Provider shall restrict physical access to facilities where PwC Data is stored or processed to its authorized Personnel by implementing industry-standard physical access controls, such as swipe card technology, monitored CCTV, remotely monitored alarm systems, on-premise security guards, photographic access credentials, visitor escort, physical access logs and authorised access lists.

Section 6—Equipment Protection

6.1 **General**. Service Provider shall store equipment storing or processing PwC Data within a dedicated, secure, and isolated facility (e.g., data centre, server room, etc.). Service Provider shall protect power and telecommunications cabling carrying PwC Data or supporting information services from interruption, interference, or damage.

6.2 **Unattended Sessions**. Service Provider shall protect unattended sessions and equipment by (a) automatically terminating or revalidating its system and application sessions; and (b) enforcing a clear desk and clear screen policy.

6.3 **Preventing Unauthorized Access**. In order to restrict unauthorized access to PwC Data, Service Provider shall (a) implement controls to protect equipment, information and assets located off-premises, including during remote access sessions, such as teleworking or remote administration; (b) publish, implement and enforce policies governing teleworking, mobile device and removable media devices; (c) encrypt remote access communications to systems or applications containing PwC Data; (d) require a minimum of multi-factor authentication Virtual Private Networking (VPN) device access or equivalent; (e) require restricted ports and protocols; PwC Data on end-user devices e.g. laptops, desktops, etc. must be encrypted; (f) Automatic device lockout must be enabled after a number of failed attempts on portable end-user devices e.g. laptops, mobile phones, etc.; (g) Remote wipe capability must be enabled on portable end-user devices (e.g. laptops, mobile phones, etc.).

6.4 **Personal Devices**. To further protect the security of PwC Data, Service Provider's policies must prohibit Personnel from accessing or storing PwC Data on any personally owned and managed equipment. Service Provider shall control Bring Your Own Device (BYOD) models, such as mobile devices and tablets, and implement controls commensurate with those on corporate-owned devices. Service Provider shall control and encrypt data on removable media devices, such as USB drives, memory sticks and Bluetooth storage devices.

6.5 **Secure Destruction**. Service Provider shall implement procedures to ensure that PwC Data is securely destroyed when no longer needed for the purposes authorized by PwC, or at the expiration or termination of the Agreement. For purposes herein, Service Provider shall (a) secure and confirm the erasure of PwC Data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal; (b) provide attestation of destruction of that PwC Data, where applicable; and (c) require that any third parties engaged to process PwC Data securely dispose of the information when no longer needed for the Services.

Section 7—Environmental Controls

7.1 **General**. Unless otherwise prohibited by Applicable Law, Service Provider shall implement, install, and

maintain the following environmental controls to protect Personnel and equipment used to process or store PwC Data: (a) fire suppression systems; (b) temperature and humidity controls within a data centre or server room environment; and (c) backup power technology (e.g., interruptible power supply, diesel generator, separate grid connection, etc.).

Section 8 – Asset Management

8.1 **Asset Register**. Service Provider shall identify and register assets that store or process PwC Data in an asset register, and at a minimum, include data location and asset ownership information.

8.2 **Asset Use**. Service Provider shall document policies for the acceptable use and handling of assets that are agreed to by its Personnel. Service Provider shall ensure that assets are immediately returned by Personnel upon termination of employment or engagement, and Service Provider shall track and verify those returned assets.

8.3 **System Hardening**. Service Provider shall implement and document system hardening procedures and baseline configurations and shall not include unsupported software or hardware.

Section 9—Communications Security

9.1 **Network Security**. Service Provider shall secure PwC Data in its network systems by implementing the following: (a) logical segregation of PwC Data within a shared service environment, and (b) securing network segments from external entry points where PwC Data is accessible.

9.2 **Network Perimeters**. Service Provider shall secure network segments from external entry points where PwC Data is accessible. Service Provider shall implement hardened configured external network perimeters to prevent unauthorized traffic and shall segment networks appropriately. Additionally, Service Provider shall: (a) protect inbound and outbound points by firewalls and intrusion detection systems (IDS); (b) limit communications to systems strictly allowed; (c) if possible, use intrusion prevention systems (IPS); (d) limit ports and protocols to those with a specific business purpose; (e) use firewalls to separate web and application servers from corresponding database servers; (f) implement access controls on wireless networks commensurate with the security level of external VPN access points using strong encryption and strong authentication (e.g., WPA2); and (g) periodically review firewall configuration (e.g., firewall ruleset, etc.).

9.3 **Internet Rules**. Service Provider shall: (a) restrict its Personnel to solely use authorized file sharing websites and tools for business purposes; (b) implement internet filtering procedures to protect end user workstations from malicious websites and unauthorized file transfers outside the network, including blocking unauthorised file sharing websites and tools; (c) implement egress filtering in place to combat unauthorised data exfiltration; (d) implement Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) when sending out emails on PwC’s behalf; and (e) enable domain-based Message Authentication Reporting and Conformance (DMARC) for handling incoming email messages.

Section 10—Cryptographic Controls

10.1 **Encryption; Information Exchange and Transfer**. Service Provider shall encrypt PwC Data (a) at rest; (b) in transit across networks, including transmission across untrusted networks, such as public networks; and (c) when writing to removable media devices. Service Provider shall obtain certificates from an authorized certification authority certifying encryption in transit. Service

Provider shall use platform and data-appropriate reasonable industry-standard encryption in non-deprecated, open, and validated formats and standard algorithms. Service Provider shall restrict the use of self-signed certificates.

10.2 **Key Management**. PwC Member Firms shall supply and govern use of the cryptographic keys, which includes the creation, rotation, and revocation of cryptographic keys. Service Provider shall segregate management duties from usage of cryptographic keys. Additionally, Service Provider shall generate and implement industry-standard cryptographic key management procedures such as approved key lengths, secure administration of keys, immediate revocation of keys upon compromise or change in user employment, recovery of lost or expired keys, backup and archive of keys, key activation and deactivation dates, and restricted access to keys.

Section 11—Service Monitoring, Testing, and Vulnerability Prevention and Remediation

11.1 **Service Management**. Service Provider shall define capacity requirements and monitor service availability.

11.2 **Penetration Testing**. Service Provider shall perform annual penetration testing for systems and applications that process PwC Data, including during significant system and application changes. Upon PwC's request, Service Provider shall provide testing results, including (a) the scope and methodology utilised; (b) the number of critical, high, and medium severity findings; (c) the name of the third-party tester; and (d) the date of the third-party testing. Service Provider shall remediate any identified vulnerability that PwC defines as "critical" risk or "high" risk in accordance with Service Provider's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management.

11.3 **Vulnerability Management**. Service Provider shall implement a patch and vulnerability management process to identify, report, test and remediate application and system vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk 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 a Risk Treatment to address identified vulnerabilities. From the date that a patch or vendor-approved workaround becomes available, Service Provider shall address vulnerabilities in accordance with Service Provider's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management. Service Provider shall implement a process in place to monitor threat intelligence to remain aware of the latest security threats.

11.4 **Malware Protection**. Service Provider shall (a) implement controls to detect and prevent malware, malicious code, and unauthorized execution of code, (b) regularly update the controls with the latest technology available (e.g., deploying the latest signatures and definitions), (c) periodically verify and/or centrally manage malware tool configurations, (d) enable real time scanning for all endpoints, including, without limitation, servers, desktops, and laptops; and (e) enable email scanning to detect malware and suspicious files.

11.5 **Logging and Monitoring**. Service Provider shall generate administrator and event logs for systems and applications that store, allow access to, or process PwC Data. The administrator and event logs must (a) be archived; (b) capture the date, time, user ID, device accessed and port used; (c) 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); (d) where technically feasible, be sent to PwC's log management tool or be made available in the case of an information security incident; and (e) be periodically reviewed by Service Provider or have alert triggers set to identify system failures, faults, or potential security incidents affecting PwC Data. Service Provider shall prevent modification of event logs and resolve or address issues with the event logs within its remediation timelines and in line with reasonable industry standards for logging and monitoring event logs.

Section 12—System Development, Acquisition, and Maintenance

12.1 **Change Control**. Service Provider shall publish and document change control procedures to manage changes to information systems, supporting infrastructure and facilities. Prior to implementing any changes, Service Provider shall (a) establish acceptance criteria for production change approval and implementation; and (b) require stakeholder approval prior to any change implementation.

12.2 **Independent Environments**. Service Provider shall maintain separate environments for development, testing and production. Service Provider shall separate and restrict Personnel access to environments with PwC Data based on Personnel job responsibilities. Additionally, Service Provider shall restrict and track Personnel access to program source code.

12.3 **Secure Development**. Service Provider shall establish, document, and integrate secure system engineering and coding practices within the system development life cycle (SDLC), and require developers to periodically attend secure system development training.

12.4 **Testing**. Service Provider shall test system and application changes, including relevant security controls. The system and application changes must meet defined acceptance criteria prior to implementation.

12.5 **Test Environment Restrictions**. Service Provider and its Personnel shall not use PwC Data meant for production within a test environment. If usage is unavoidable, Service Provider shall (a) mask PwC Data by obfuscation, Sanitization, de-identification or anonymization; or (b) the test environment shall have security controls equivalent to those within the production environment.

12.6 **Source Code**. Unless otherwise agreed to by PwC, Service Provider shall implement automated static source code analysis and vulnerability remediation prior to the initial transfer of any PwC Data into Service Provider's environment, 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. Following any system changes, Service Provider shall perform post-implementation testing to confirm that existing applications and security controls were not compromised.

12.7 **Monitoring**. Service Provider shall validate that outsourced system development activities follow policies and processes aligned with Service Provider's information security requirements.

Section 13—Third-party Service Provider Management

13.1 **Flow-down Terms**. Service Provider shall include in its agreements with third parties processing PwC Data information security, confidentiality, and data protection requirements similar to the provisions in the Agreement. Service Provider shall ensure that it and those third parties shall periodically review (a) the agreements to validate those requirements, and (b) the third parties' information security and data protection requirements to validate the appropriateness of the requirements to the risks represented by the third parties' processing of PwC Data.

13.2 **Third-party Access to PwC Data**. Service Provider shall provide third parties access to PwC Data solely when necessary to perform the Services. In those cases, Service Provider shall (a) provide the PwC Member Firm a list of third parties with access to PwC Data; (b) limit third party access to PwC Data only as necessary to perform the Services as contractually agreed to between the third parties and Service Provider; and (c) record third party access to PwC Data within system logs, subject to Service Provider controls for logging and monitoring. Unless otherwise provided herein, Service Provider shall restrict third party access to PwC Data.

Section 14—Incident Management

14.1 **Incident Management Policy**. Service Provider shall implement a formally documented incident management policy that includes: (a) clearly defined management and user roles and responsibilities; (b) a reporting mechanism for incidents and events affecting the security of PwC Data, including the reporting of suspected unauthorised or unlawful access, disclosure, loss, alteration and destruction of PwC Data; (c) procedures for Risk Assessments and Risk Treatments 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 Applicable Law and the PwC Member Firms; (e) procedures for forensic investigation of a security incident; (f) processes for incident and resolution analysis designed to prevent the same, or similar, incidents from repeating; and (g) reporting suspected unauthorised or unlawful access, disclosure, loss, alteration, and/or destruction of PwC Data to PwC without undue delay.

14.2 **Incident Tracking System**. Service Provider shall maintain a security incident tracking system for PwC Data that documents and describes relevant information for each security incident affecting PwC Data throughout its life cycle, such as incident details, whether there was a data breach, the data affected, and remediation actions taken.

14.3 **Investigations**. Service Provider shall support any investigation by PwC, law enforcement, or regulatory authorities that involves PwC Data by developing forensic procedures to support incident investigation.

Section 15—Resilience

15.1 **Business Continuity, Disaster Recovery**.

(a) **General**. Service Provider shall perform business continuity Risk Assessments to determine relevant risks, threats, likelihood of a service outage or Data Breach, impacts of a service outage or Data Breach, and required controls and procedures to secure PwC Data. Based on Risk Assessment results, Service Provider shall document, implement, annually test and review business continuity and disaster recovery plans to validate the ability to timely restore availability and access to PwC Data in the event of a service outage or Data Breach (a "**BCDR Plan**"). In its business continuity and disaster recovery plan, Service Provider shall include (a) availability requirements for PwC Member Firm services, specifying critical systems; (b) agreed upon recovery points (RPO) and recovery time objectives (RTO); (c) clearly defined roles and responsibilities; (d) provisions for a geographically separate site subject to physical and environmental controls; and (e) backup and restoration procedures that include sanitation, disposal, or destruction of data stored at the alternate site.

(b) **Implementing the BCDR Plan**. A "**Disaster**" means any event that causes the unplanned interruption, inaccessibility, or unavailability of any or all of the Services for 30 minutes or longer. In the event of a Disaster, Service Provider shall (i) notify PwC within 1 hour of the Disaster, (ii) implement the BCDR Plan within 2 hours of the Disaster, and (iii) fully restore the Services within 12 hours of the Disaster. Service Provider shall provide PwC with no less resource allocation priority than Service Provider's other customers. Service Provider shall not charge any additional fees or expenses for implementation the BCDR Plan.

(c) **Root Cause Analysis**. Following each Disaster after the Services have been fully restored, Service Provider shall conduct a root cause analysis and provide to PwC a comprehensive report that describes, at a minimum, (i) the cause or causes of the Disaster, (ii) efforts taken to mitigate the consequences and resolve the Disaster, and (iii) the remedial actions to be implemented by Service Provider in order to avoid future Disasters.

15.2 **Backup Procedures and Media**. Service Provider shall follow industry best practices to make regular, encrypted backups of database and repository files of PwC Data to a secured location separate from the primary data centre, on a timeframe mutually agreed to by the parties. Information backup procedures and media must include (a) strong encryption technology; (b) integrity validation; (c) reconciliation with disaster recovery requirements; and (d) secure offsite storage supporting availability requirements. Service Provider shall restore any corrupted files using the most current backup available.

Section 16—Audit and Compliance

16.1 **Compliance**. Service Provider shall periodically review its systems and equipment storing, enabling access to, or otherwise processing PwC Data, compliance with Applicable Law and contractual obligations owed to PwC. Service Provider management shall annually review the technical and organisational controls implemented to protect PwC Data and comply with contractual obligations, and report results to Service Provider senior management.

16.2 **PwC Assessment**. Service Provider shall allow PwC to monitor and assess Service Provider's adherence to contractual requirements under the Agreement, including information security controls.

(a) **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., ProcessUnity or similar tool). Service Provider shall make relevant documentation, reports, and evidence available for review upon PwC's request. Service Provider shall cooperate with PwC to remediate issues identified in an online security ratings service (e.g., BitSight or similar tool).

16.3 **Audit Reports**. Service Provider shall maintain independent verification of the effectiveness of its technical and organizational security measures. Service Provider shall cause an independent third party to at least annually conduct an audit and produce a SOC 2 Type 2 Report covering the prior 12-month period. Service Provider shall make available to PwC the current SOC 2 Type 2 Report, including the status of any exceptions identified within the SOC 2 Type 2 Report. Service

Provider shall also comply with the controls in, and maintain, an ISO 27001 Certification, providing that certification and a copy of Service Provider's Statement of Applicability (SOA) to PwC upon its request.

16.4 **Remediation**. Promptly following the completion of each of the audits, assessments, reports, or tests described in **Sections 16.1** through **16.3**, Service Provider shall prioritize remediation efforts according to the severity of the identified vulnerabilities and take prompt action to address all identified "critical" or "high" vulnerabilities. Service Provider will remediate vulnerabilities in accordance with Service Provider's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management. 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.

16.5 **Disclosure**. Without the need for confidentiality measures, PwC may share the results of any audit, report, or test under this **Section 16** with any PwC Member Firm or any government regulator of any PwC Member Firm. Under appropriate confidentiality measures, PwC may share the results of any audit, report, or test under this **Section 16** with actual or prospective clients of any PwC Member Firm. 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.

Section 17—Termination of Services

17.1 **General**. Service Provider shall comply with a documented termination or conclusion of Service process. Non-disclosure and confidentiality responsibilities with respect to PwC Data shall remain in place following Agreement or Order termination or conclusion. Service Provider shall identify a primary point of contact to support the Service termination process and communicate that termination or conclusion to relevant Personnel and stakeholders. Additionally, Service Provider shall (a) revoke access to systems and applications storing, allowing access to, or processing PwC Data promptly upon completion or termination of the Agreement or Order; (b) return hardware, software, middleware, documents, data, information, and other assets owned or leased from the PwC Member Firm; and (c) confirm the return or destruction of all copies of PwC Data in Service Provider's possession or control, including any information stored on backup media to PwC.