ACCENTURE'S INFORMATION SECURITY SUPPLIER SECURITY REQUIREMENTS
MARCH 2022

Provider agrees it has implemented and will maintain throughout the term of the Agreement and all Orders and Statements of Work the following technical and organizational measures, controls, and information security practices:

1. **Information Security Policies**
   a. **Policies for Information Security.** Provider's policies for information security shall be documented by Provider, approved by Provider's management, published, and communicated to Provider's personnel, contractors, agents and relevant external third parties.
   b. **Review of the Policies for Information Security.** Provider information security policies shall be reviewed by Provider at least annually, or promptly after material changes to the policies occur, to confirm applicability and effectiveness.
   c. **Information Security Reviews.** The Provider's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

2. **Organization of Information Security**
   a. **Security Accountability.** Provider shall assign one or more security officers who will be responsible for coordinating and monitoring Provider's information security function, policies, and procedures.
   b. **Security Roles and Responsibility**. Provider personnel, contractors and agents who are involved in providing Provider Services shall be subject to confidentiality agreements with Provider.
   c. **Risk Management**. Appropriate information security risk assessments shall be performed by Provider as part of an ongoing risk governance program that is established with the objective to recognize risk; to assess the impact of risk; and where risk reducing or mitigation strategies are identified and implemented, to effectively manage the risk with recognition that the threat landscape constantly changes.

3. **Human Resource Security**
   a. **Security Training.** Appropriate security awareness, education and training shall be provided to all Provider personnel and contractors.

4. **Asset Management**
   a. **Asset Inventory.** Provider shall maintain an asset inventory of all media and equipment where Accenture Data is stored. Access to such media and equipment shall be restricted to authorized personnel of Provider. Provider will ensure that no software or hardware that is past its End of Life (EOL) will be used in the scope of Provider Services without a mutually agreed risk management process for such items.
   b. **Asset Handling**
      i. Provider shall classify Accenture Data so that it is properly identified and access to Accenture Data shall be appropriately restricted.
      ii. Provider shall maintain an acceptable use policy with restrictions on printing Accenture Data and procedures for appropriately disposing of printed materials that contain Accenture Data when such data is no longer needed to provide the Provider Services under the Agreement.
      iii. Provider shall maintain an appropriate approval process whereby such approval is provided to personnel, contractors, and agents prior to storing Accenture Data on portable devices; remotely accessing Accenture Data; or processing such data outside of Provider facilities. If storing Accenture Data on portable devices is approved and granted, Provider shall enforce the use of current Industry Standard encryption on the portable device. If mobile devices

are used to access or store Accenture Data, Provider personnel, contractors and agents shall use a mobile device management (MDM)/mobile application mangement (MAM) solution that enforces encryption, passcode, and remote wipe settings to secure Accenture Data. Provider will prohibit the enrollment of mobile devices that have been "jail broken."

5. **Access Control.** Provider shall maintain an appropriate access control policy that is designed to restrict access to Accenture Data and Provider assets to authorized personnel, agents, and contractors.

a. Authorization

i. Provider shall maintain user account creation and deletion procedures for granting and revoking access to all assets, Accenture Data, and all internal applications while providing Provider Services under the Agreement. The Provider will assign an appropriate authority to approve creation of user accounts or elevated levels of access for existing accounts.

ii. Provider shall maintain and update records of personnel who are authorized to access Provider systems that are involved in providing Provider Services and review such records at least quarterly.

iii. Provider shall ensure the uniqueness of user accounts and passwords for each individual. Individual user accounts must not be shared.

iv. Provider shall remove access rights to assets that store Accenture Data for personnel, contractors and agents upon termination of their employment, contract or agreement within two (2) business days, or access shall be appropriately adjusted upon change (e.g., change of personnel role).

v. Provider will perform periodic access reviews for system users at least quarterly for all supporting systems requiring access control.

b. Least Privilege Access

i. Provider shall restrict access to Provider systems involved in providing Provider Services, to only those individuals who require such access to perform their duties using the principle of least privilege access.

ii. Administrative and technical support personnel, agents or contractors shall only be permitted to have access to such data when required.

iii. Provider shall support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., programming/administrator, developer/operations).

c. Authentication

i. Provider will use current, and at a minimum, Industry Standard capabilities to identify and authenticate personnel, agents and contractors who attempt to access information systems and assets.

ii. Provider shall maintain current Industry Standard practices to deactivate passwords that have been corrupted or disclosed.

iii. Provider shall monitor for repeated access attempts to information systems and assets.

iv. Provider shall maintain current Industry Standard password protection practices that are designed and in effect to maintain the confidentiality and integrity of passwords generated, assigned, distributed, and stored in any form.

v. Provider shall provide an Industry Standards based single sign-on (SSO) capability (SAML, Open Authorization (Oauth v2), etc.) which will support integration with Accenture's SSO solutions to enable authentication to access any Provider web-based application(s) provided as part of the Provider Services, unless the requirement is explicitly waived by Accenture. Details of how the single sign-on integration must be implemented are available from Accenture upon request. If SSO is not implemented due to technical limitations or Accenture requirements, multi-factor authentication will be required for access to Provider web-based application(s) provided as part of the Provider Services.

vi. Provider shall maintain and enforce a password policy that is aligned to current Industry Standards (e.g., NIST Cyber Security Framework, PCI DSS (Payment Card Industry Data Security Standard), Center for Internet Security) and default passwords must be changed before deploying any new asset. In the event that Provider Services includes the management of Accenture or its client infrastructure and environments, account lockout

thresholds must be consistent with Accenture or its client account lockout standards, whichever is most strict.

vii. Provider personnel, agents and contractors shall use multi-factor authentication and encrypted sessions for access to Provider systems. In the event that Provider Services require external connections to Accenture or Accenture client project dedicated environments, Accenture must provide approval of the connections.

6. **Cryptography.** Provider shall maintain policies and standards regarding the use of cryptographic controls that are implemented to protect Accenture Data. Provider shall implement Industry Standard key management policies and practices designed to protect and generate encryption keys for their entire lifetime.

7. **Physical and Environmental Security**
   a. **Physical Access to Facilities.** Provider shall limit access to facilities (where systems that are involved in providing the Provider Services are located) to identified personnel, agents and contractors.
   b. **Physical Access to Components.** Provider shall maintain records of incoming and outgoing media containing Accenture Data, including the type of media, the authorized sender/recipient, the date and time, the number of media, and the type of data the media contains. Provider shall ensure that backups (including remote and cloud service backups) are properly protected via physical security or encryption when stored, as well as when they are moved across the network. In the event that backup media of Accenture and/or Accenture client data is stored / shipped offsite, Accenture must provide approval of the storage location.
   c. **Protection from Disruptions.** The Provider shall protect equipment from power failures and other disruptions caused by failures in supporting utilities. Telecommunications and network cabling must be protected from interception, interference, and/or damage.
   d. **Secure Disposal or Reuse of Equipment.** Provider shall verify equipment containing storage media, to confirm that all Accenture Data has been deleted or securely overwritten using Industry Standard processes, prior to disposal or re-use.
   e. **Clear Desk and Clear Screen Policy**. Provider shall adopt a clear desk policy for papers and removable storage media and a clear screen policy.

8. **Operations Security**
   a. **Operations Policy.** Provider shall maintain appropriate operational and security operating procedures and such procedures shall be made available to all personnel who require them.
   b. **Logging and Monitoring of Events**
      i. Provider must enable logging and monitoring on all operating systems, databases, applications, and security and network devices that are involved in providing Provider Services. Logs must be kept for a minimum of 6 months or as long as legally required, whichever is longer. Logs must capture the access ID, the authorization granted or denied, the date and time, the relevant activity, and be regularly reviewed. All relevant information processing systems shall synchronize time to a single reference time source.
      ii. Logging capabilities shall be protected from alteration and unauthorized access.
   c. **Protections from Malware.** Provider shall maintain anti-malware controls that are designed to protect systems from malicious software, including malicious software that originates from public networks. Provider shall maintain software at the then current major release for Provider owned anti-malware software and shall maintain appropriate maintenance and support for new releases and versions of such software.
   d. **Encrypted Backup**. Provider shall maintain an encrypted backup and restoration policy that also protects Accenture Data from exposure to ransomware attacks, and shall back up Accenture Data, software, and system images in accordance with Provider policy unless other such requirements are agreed upon. Provider shall regularly test restoration procedures.
   e. **Control of Software and Utilities.** Provider shall enforce policies and procedures that govern the installation of software and utilities by personnel.

f. **Change Management.** Provider shall maintain and implement procedures to ensure that only approved and secure versions of code, configurations, systems, utilities, and applications will be deployed for use.

g. **Encryption of Data at Rest**. Provider shall encrypt data at rest, including data at rest in cloud instances and storage buckets, using current Industry Standard encryption solutions or shall provide the capability with instructions to Accenture so that Accenture may enable further encryption, at Accenture's discretion.

9. Communications Security

a. **Information Transfer and Storage.**
   i. Provider shall use current Industry Standard encryption, TLS (Transport Layer Security) minimum version 1.2, to encrypt Accenture Data that is in transit.
   ii. Provider shall use TLS, minimum version 1.2, over SMTP (Simple Mail Transfer Protocol) when exchanging emails as a standard practice to encrypt emails in transit.
   iii. Provider shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy of reject to lower the chance of spoofed or modified emails from valid domains. This is required for email that is sent from Provider applications.
   iv. In the event that Provider Services include the management of Accenture client email systems, such systems must be configured and implemented to agreed-upon standards.
   v. Provider shall utilize a secure collaboration platform that is enabled to restrict access and encrypt communications and Accenture Data.
   vi. Provider shall restrict access through encryption to Accenture Data stored on media that is physically transported from Provider facilities.

b. **Security of Network Services.** Provider shall ensure that Industry Standard security controls and procedures for all network services and components are implemented whether such services are provided in-house or outsourced. In the event that Provider Services include the management of network services and components owned by Accenture or its client, such services and components must be configured and implemented to agreed-upon standards.

c. **Intrusion Detection.** Provider shall deploy intrusion detection and intrusion prevention systems to provide continuous surveillance for intercepting and responding to security events as they are identified and update the signature database as soon as new releases become available for commercial distribution.

d. **Firewalls.** Provider shall have appropriate firewalls in place which will only allow documented and approved ports and services to be used. All other ports will be in a deny all mode.

e. **Web Filtering.** Provider shall have a Web filtering policy in place to control the content that users can access over the Internet. This includes restricting the use of personal emails and file sharing sites.

f. **Data Loss Prevention.** Provider shall have a data loss prevention policy in place to monitor for or restrict the unauthorized movement of Accenture Data.

10. System Acquisition, Development and Maintenance

a. **Workstation Encryption.** Provider will require Industry Standard full disk encryption on all workstations and/or laptops used by personnel, contractors and agents where such personnel are accessing or processing Accenture Data.

b. **Application Hardening.**
   i. Provider will maintain and implement secure application development policies, procedures, and standards that are aligned to Industry Standard practices such as the SANS Top 25 Software Errors, the OWASP Top Ten project and the NIST Secure Software Development Framework (SSDF). This applies to web application, mobile application, embedded software, and firmware development as appropriate.
   ii. All personnel responsible for secure application design, development, configuration, testing, and deployment will be qualified to perform the Provider Services and receive appropriate training regarding Provider's secure application development practices.

c. **System Configuration and Hardening.**

i. Provider will establish and ensure the use of Industry Standard secure configurations of technology infrastructure. Images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated on a regular basis to update their security configuration as appropriate.
ii. Provider will perform periodic access reviews for system administrators at least quarterly for all supporting systems requiring access control.
iii. Provider will implement patching tools and processes for operating systems and applications installed on the system. Provider shall have a defined process to remediate findings and will ensure that emergency/critical issues are addressed urgently and as soon as practicable within fourteen (14) days; high-risk issues are addressed within thirty (30) days; and medium-risk issues are addressed within ninety (90) days. When outdated systems can no longer be patched, Provider will update to the latest supported version of the operating system and applications installed on the system. If this is not possible, Provider shall purchase extended support and notify Accenture so that an appropriate risk assessment can be conducted. Provider will remove outdated, older, and unused software from the system. In the event that Provider Services include patch management for operating systems and applications owned by Accenture or its client, Provider shall document and implement an appropriate patching plan that includes agreed-upon remediation service level obligations.
iv. Provider will limit administrative privileges to only those personnel who have both the knowledge necessary to administer the operating system and a business need to modify the configuration of the underlying operating system.

d. Infrastructure Vulnerability Scanning. Provider shall use Industry Standard and up-to-date products to scan its internal and external environment (e.g., servers, network devices, etc.) related to Provider Services on a quarterly basis. Provider shall have a defined process to remediate findings and will ensure that emergency/critical issues are addressed urgently and as soon as practicable within fourteen (14) days; high-risk issues are addressed within thirty (30) days; and medium-risk issues are addressed within ninety (90) days. In the event that Provider Services include infrastructure vulnerability management for infrastructure owned by Accenture or its client, Provider shall document and implement an infrastructure scanning and vulnerability remediation plan that is to be approved by Accenture.

e. Application Vulnerability Assessment. Provider will perform application security vulnerability assessments prior to any release and on a recurring basis. The assessments must cover all web application, mobile application, stand-alone application, embedded software, and firmware vulnerabilities defined by the Open Web Application Security Project (OWASP) or those listed in the SANS Top 25 Software Errors or its successor current at the time of the test. Provider will ensure all critical and high-risk vulnerabilities are remediated prior to release. On a recurring basis, Provider shall ensure that emergency/critical vulnerabilities are addressed urgently and as soon as practicable within fourteen (14) days; high-risk vulnerabilities are addressed within thirty (30) days; and medium-risk vulnerabilities are addressed within ninety (90) days. This applies to web application, mobile application, stand-alone application, embedded software, and firmware development as appropriate to the Agreement. In the event that Provider Services include application vulnerability management for applications owned by Accenture or its client, Provider shall document and implement an application vulnerability assessment and remediation plan that is to be approved by Accenture.

f. Penetration Tests and Security Evaluations of Websites. Provider shall use an established Industry Standard program to perform external and internal penetration tests and security evaluations of all systems and websites involved in providing Provider Services prior to use and on a recurring basis no less frequently than once in a twelve (12)-month period by an industry recognized independent third party. Provider shall have a defined process to remediate findings and will ensure that emergency/critical issues are addressed urgently and as soon as practicable within fourteen (14) days; high-risk vulnerabilities are addressed within thirty (30) days; and medium-risk issues are addressed within ninety (90) days.

g. Supporting Documentation. Upon Accenture request, Provider shall provide a summary of vulnerability scans, penetration tests and/or any security evaluations conducted, including any open remediation points. In the absence of such summaries, documentation sufficient to prove that such scans have been conducted shall be provided.

h. Separation of Environments. Provider shall maintain separate environments for production and non-production systems and developers should not have unmonitored access to production environments.

11. Provider Relationships

a. Where other third-party applications or services must be engaged by Provider, Provider's contract with any third-party must clearly state appropriate security requirements substantially similar to this Information Security Schedule. In addition, service level agreements with the third party must be clearly defined.

b. Any external third-party or resources gaining access to systems must be covered by a signed agreement containing confidentiality language consistent with the confidentiality and security requirements of the Agreement.

c. Provider shall regularly conduct security reviews of third-party suppliers to address physical and logical security requirements, privacy protection, breach reporting, and contractual requirements. Provider shall ensure that all findings from such security reviews are promptly remediated.

d. Provider will perform quality control and security management oversight of outsourced software development.

12. Information Security Incident Management

a. Incident Response Process

i. Provider shall maintain a record of Security Incidents noting the description of the Security Incident, the applicable time periods, the impact, the person reporting and to whom the Security Incident was reported, and the procedures to remediate the incident.

ii. In the event of a Security Incident identified by Provider, Accenture, or other third party, Provider will: (a) promptly investigate the Security Incident; (b) promptly provide Accenture with all relevant detailed information as reasonably requested by Accenture about the Security Incident; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

iii. The Provider shall track disclosures of Accenture Data, including what type of data was disclosed, to whom, and the time of the disclosure.

13. Compliance

a. Legal and Contractual Requirements.

i. Provisions regarding compliance with laws, intellectual property and data privacy are contained in the body of the Agreement and applicable schedules.

SUPPLEMENTARY MEASURES. In addition, in accordance with regulatory guidance following the European Court of Justice "Schrems II" decision, Supplier further commits to maintaining the following additional technical, organizational and legal/contractual measures with respect to Accenture Data, including personal data.

Technical Supplementary Measures:

Accenture Data in transit between Supplier entities will be strongly encrypted with encryption that:

- **b.** is state of the art,
- **c.** secures the confidentiality for the required time period,
- **d.** is implemented by properly maintained software,
- **e.** is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and
- **f.** does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.

Accenture Data at rest and stored by any Supplier entities will be strongly encrypted with encryption that:

- **g.** is state of the art,
- **h.** secures the confidentiality for the required time period,
- **i.** is implemented by properly maintained software,
- **j.** is robust and provides protection against active and passive attacks by public authorities, including crypto analysis, and
- **k.** does not contain back doors in hardware or software, unless otherwise agreed with the applicable Client.