RESPONSIV DATA SECURITY AND PRIVACY PRINCIPLES

1. Definitions

Capitalised terms used herein have the meanings given below or if not defined below, the meanings given in the applicable written contract between Responsiv and Customer for the Responsiv Services.

Customer – is the entity to which Responsiv is providing the Responsiv Services under a Responsiv Services Document.

Components – are the application, platform, or infrastructure elements of a Responsiv Service that Responsiv operates and manages.

Content – consists of all data, software, and information that Customer or its authorised users provide, authorise access to, or input to Responsiv Services.

DSPP – is this Responsiv Data Security and Privacy Principles document.

Responsiv Cloud Services – are "as a service" Responsiv offerings that Responsiv makes available via a network, such as software as a service, platform as a service, or infrastructure as a service.

Responsiv Services Document – is a Transaction Document and any other document that is incorporated into a written contract between Responsiv and a Customer and that addresses details of a specific Responsiv Service.

Responsiv Services – are (a) Responsiv Cloud Services, (b) other Responsiv service offerings, including infrastructure or application service offerings that Responsiv delivers and dedicates to or customises for a Customer, and (c) any other services, including consulting, maintenance, or support, that Responsiv provides to a Customer.

Security Incident – is an unauthorised access and unauthorised use of Content.

Transaction Document – is a document that details the specifics of transactions, such as charges and a description of and information about a Responsiv Cloud Service. Examples of Transaction Documents include statements of work, service descriptions, ordering documents and invoices for a Responsiv Cloud Service. There may be more than one Transaction Document applicable to a transaction.

2. Overview

The technical and organisational measures provided in this DSPP apply to Responsiv Services (including any Components) only where Responsiv has expressly agreed to comply with the DSPP in a written contract between Responsiv and Customer. For clarity, those measures do not apply where Customer is responsible for security and privacy or as specified below or in a Responsiv Services Document.

2.1. Customer is responsible for determining whether a Responsiv Service is suitable for Customer's use and implementing and managing security and privacy measures for components that Responsiv does not provide or manage within the Responsiv Services. Examples of Customer responsibilities for Responsiv Services include: (1) the security of systems and applications built or deployed by the Customer upon an infrastructure as a service or platform as a service offering or upon infrastructure, Components or software that Responsiv manages for a Customer, and (2) Customer end-user access control and application level security configuration for a software as a service offering that Responsiv manages for a Customer or an application service offering that Responsiv delivers to a Customer.

2.2. Customer acknowledges that Responsiv may modify this DSPP from time to time at Responsiv's sole discretion and such modifications will replace prior versions as of the date that Responsiv publishes the modified version. Notwithstanding anything to the contrary in any written contract between Responsiv and Customer, the intent of any modification will be to: (1) improve or clarify existing commitments, (2) enable Responsiv to appropriately prioritise its security focus to address evolving data and cybersecurity threats and issues, (3) maintain alignment to current adopted standards and applicable laws, or (4) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of Responsiv Services.

2.3. In the event of any conflict between this DSPP and a Responsiv Services Document, the Responsiv Services Document will prevail and if the conflicting terms are in a Transaction Document, they will be identified as overriding the terms of this DSPP and will only apply to the specific transaction.

3. Data Protection

3.1. Responsiv will treat all Content as confidential by not disclosing Content except to Responsiv employees, contractors, and suppliers (including sub-processors), and only to the extent necessary to deliver the Responsiv Services.

3.2. Security and privacy measures for each Responsiv Service are implemented in accordance with Responsiv's security and privacy by design practices to protect Content processed by a Responsiv Service, and to maintain the availability of such Content pursuant to the applicable written contract between Responsiv and Customer, including applicable Responsiv Services Documents.

3.3. Additional security and privacy information specific to a Responsiv Service may be available in the relevant Responsiv Services Document or other standard documentation to aid in Customer's initial and ongoing assessment of a Responsiv Service's suitability for Customer's use. Responsiv will direct Customer to available standard documentation if asked to complete Customer-preferred security or privacy questionnaires.

4. Security Policies

4.1. Responsiv will maintain and follow written IT security policies and practices that are integral to Responsiv's business and mandatory for all Responsiv employees. The Responsiv Chief Operating Officer will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

4.2. Responsiv will review its IT security policies at least annually and amend such policies as Responsiv deems reasonable to maintain protection of Responsiv Services and Content.

4.3. Responsiv will maintain and follow its standard mandatory employment verification requirements for all new hires. In accordance with Responsiv internal processes and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by Responsiv.

4.4. Responsiv employees will complete Responsiv's security and privacy education annually. Additional training will be provided to any persons granted privileged access to Components that is specific to their role within Responsiv's operation and support of the Responsiv Services, and as required to maintain compliance and accreditations stated in any relevant Responsiv Services Document

5. Compliance

5.1. For standard (non-custom) Responsiv Cloud Services, the measures implemented and maintained by Responsiv within each Responsiv Cloud Service will be subject to annual review and where applicable, penetration tests.

5.2. Additionally, Responsiv will maintain compliance and accreditation for the Responsiv Services as defined in a Responsiv Services Document.

5.3. Upon request, Responsiv will provide evidence of the compliance and accreditation required by 5.1. and 5.2, such as certificates, attestations, or reports resulting from accredited independent third-party audits (accredited independent third-party audits will occur at the frequency required by the relevant standard).

5.4. Responsiv is responsible for these data security and privacy measures even if Responsiv uses a contractor or supplier (including sub-processors) in the delivery or support of a Responsiv Service.

6. Security Incidents

6.1. Responsiv will maintain and follow documented incident response policies consistent with industry standard practices or equivalent industry standards for computer security incident handling and will comply with the data breach notification terms of the applicable written contract between Responsiv and Customer.

6.2. Responsiv will investigate Security Incidents of which Responsiv becomes aware, and, within the scope of the Responsiv Services, Responsiv will define and execute an appropriate response plan. Customer may notify Responsiv of a suspected vulnerability or incident by submitting a request through the incident reporting process specific to the Responsiv Service (as referenced in a Responsiv Services Document) or, in the absence of such process, by submitting a technical support request.

6.3. Responsiv will notify Customer without undue delay upon confirmation of a Security Incident that is known or reasonably suspected by Responsiv to affect Customer. Responsiv will provide Customer with reasonably requested information about such Security Incident and the status of any Responsiv remediation and restoration activities

7. Physical Security and Entry Control

7.1. Responsiv Services are hosted on industry recognised cloud platforms including, but not limited to, IBM Cloud, Microsoft Azure, Amazon AWS, Google Cloud. All physical security and entry controls will be managed by our cloud platform providers in line with their published policies. Responsiv will assist Customers identify information relating to the policies published by our cloud platform providers in this area so that the Customer can assure themselves of the suitability of the platform to meet their specific requirements

8. Access, Intervention, Transfer and Separation Control

8.1. Responsiv will maintain a documented security architecture for Components. Responsiv will separately review such security architecture, including measures designed to prevent unauthorised network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense-in-depth standards prior to implementation.

8.2. Responsiv may use wireless networking technology in its maintenance and support of the Responsiv Services and associated Components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to Responsiv Cloud Services networks. Responsiv Cloud Services networks do not use wireless networking technology.

8.3. Responsiv will maintain measures for a Responsiv Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorised persons. Responsiv will maintain appropriate isolation of its

production and non-production environments, and, if Content is transferred to a non- production environment, for example to reproduce an error at Customer's request, security and privacy protections in the non-production environment will be equivalent to those in production.

8.4. Responsiv will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use whenever possible of a cryptographic protocol, such as HTTPS, SFTP, or FTPS, for Customer's secure transfer of Content to and from the Responsiv Services over public networks.

8.5. If requested by the Customer and to the extent supported by the products, Responsiv will encrypt Content at rest and restrict access using ACL if and as specified in a Responsiv Services Document. If a Responsiv Service includes management of cryptographic keys, Responsiv will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

8.6. If Responsiv requires access to Content to provide the Responsiv Services, and if such access is managed by Responsiv, Responsiv will restrict access to the minimum level required. Such access, including administrative access to any underlying Components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorised Responsiv personnel following the principles of segregation of duties. Responsiv will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or upon the request of authorised Responsiv personnel, such as the account owner's manager.

8.7. Consistent with industry standard practices, and to the extent natively supported by each Component, Responsiv will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, password change frequency, and secure transfer and storage of such passwords and passphrases.

8.8. Logs in which privileged access and activity are recorded will be retained in compliance with Responsiv's records management plan. Responsiv will maintain measures designed to protect against unauthorised access, modification, and accidental or deliberate destruction of such logs.

8.9. To the extent supported by native device or operating system functionality, Responsiv will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

9. Service Integrity and Availability Control

9.1. Responsiv will: (1) perform security and privacy risk assessments of the Responsiv Services at least annually, (2) perform security testing and vulnerability assessments of the Responsiv Services before production release and at least annually thereafter, (3) enlist a qualified independent third party, or, if specified in a Responsiv Services Document, another qualified testing service to perform penetration testing of the Responsiv Cloud Services, at least annually, (4) perform automated vulnerability scanning of underlying Components of the Responsiv Services against industry security configuration best practices, (5) remediate identified vulnerabilities from security testing and scanning, based on associated risk, exploitability, and impact, and (6) take reasonable steps to avoid disruption to the Responsiv Services when performing its tests, assessments, scans, and execution of remediation activities.

9.2. Responsiv will maintain measures designed to assess, test, and apply security advisory patches to the Responsiv Services and associated systems, networks, applications, and underlying Components within the scope of the Responsiv Services. Upon determining that a security advisory patch is applicable and appropriate, Responsiv will implement the patch pursuant to severity and risk assessment guidelines, based on Common Vulnerability Scoring System ratings of patches, when available. Implementation of security advisory patches will be subject to Responsiv change management policy.

9.3. Responsiv will maintain policies and procedures designed to manage risks associated with the application of changes to Responsiv Services. Prior to implementation, changes to a Responsiv Service, including its systems, networks, and underlying Components, will be documented in a registered change request that includes a description of and reason for the change, implementation details and schedule, a risk statement addressing impact to the Responsiv Service and its clients, expected outcome, rollback plan, and documented approval by authorised personnel.

9.4. Responsiv will maintain an inventory of all information technology assets used in its operation of Responsiv Services. Responsiv will continuously monitor and manage the health, including capacity, and availability of Responsiv Services and underlying Components.

9.5. Each Responsiv Service will be separately assessed for business continuity and disaster recovery requirements through appropriate business impact analysis and risk assessments intended to identify and prioritise critical business functions. Each Responsiv Service will have, to the extent warranted by such risk assessments, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for a Responsiv Service, if provided for in the relevant Responsiv Services Document, will be established with consideration given to the Responsiv Service's architecture and intended use.