verian

Supplier Information Security Obligations

1. INTRODUCTION

The basic requirements for Supplier information security, as needed to ensure the confidentiality, availability and integrity of Customer Confidential and Restricted Information are established by these Information Security Obligations. During the Supplier's performance of services under this Agreement the Supplier shall comply with these requirements.

2. TERMINOLOGY

The terms below (whether used with initial upper case or in all lower case) shall have the corresponding meaning as described. Each other capitalised term used herein but not defined herein shall have the meaning ascribed to it in this Agreement.

Contractor means a subcontractor, independent contractor, service provider or agent of Supplier that stores, processes, handles or has access to any Customer Confidential Information or Customer Restricted Information.

Customer means the Verian Group legal entity specified in the PO in the "Bill to" field.

Customer Confidential Information means any Customer Confidential Information that does not include Personal Information [email, name etc.], health information, financial information, or investment holdings information, for example Supplier briefing documents, internal business data e.g. strategy, audit reports, pre-release marketing information, Customer proprietary software or business continuity infrastructure plans.

Customer Data means any Customer Confidential Information or Customer Restricted Information.

Customer Restricted Information means any Customer Confidential Information that includes Personal Information [email, name etc.], health information, financial information, or investment holdings information.

Encryption means the reversible transformation of data from the original format (plaintext) to an obfuscated format (ciphertext) as a method for protecting the information's confidentiality, integrity and/or authenticity. Encryption involves an encryption algorithm and one or more encryption keys.

PO means the purchase order issued by the Customer and accepted by the Supplier that incorporates these Conditions by reference.

Store means to store, archive, back-up and/or carry out any similar activities.

Supplier means the Supplier specified in the PO.

PART A - DATA SECURITY OBLIGATIONS

1. To prevent unauthorised access to any system or information used in connection with this Agreement, the Supplier shall employ and maintain reasonable physical and electronic security measures;

2. To protect against commonly known threats, the Supplier shall maintain up to date antivirus definitions and security patches for all systems and software;

3. The Supplier shall promptly inform the Customer of any security breach or lapse in security that might adversely affect the Customer, including, but not limited to, any unauthorised access to or compromise of any Customer Data or the systems put in place between the parties to transfer and/or provide access to Customer Data;

4. All Customer Restricted Information shall be transmitted and stored by the Supplier in an encrypted format using algorithms listed in "Part C - Customer Supplier Information Protection Guidelines" below; The Supplier shall implement security key management and other facilities to ensure that encrypted Customer Restricted Information is not lost or irretrievable should the encryption keys become unavailable;

5. A firewall for all systems and Internet connection points shall be maintained by the Supplier, with access control restricted to that required for authorised use of the systems and applications in connection with this Agreement;

6. To protect against unauthorised access to any device used to access systems and applications in connection with this Agreement the Supplier shall provide physical security;

7. Functional and current antivirus and firewall software should be installed on all remote personal computing systems, workstations and laptops that access systems and applications in connection with this Agreement and appropriate security patches should be applied;

8. The Supplier shall not try to exceed the permitted access to a system or application authorised by the Customer in connection with this Agreement.

9. An information security programme ("Security Programme") shall be maintained by the

Supplier that has administrative, technical, and physical safeguards that are appropriate for its size and complexity, the nature and scope of its activities and the sensitivity of Customer Data transmitted or received in connection with this Agreement. Regarding its obligations under this Agreement, the Supplier shall comply with and adhere to its Security Programme and shall, upon request by the Customer, provide the Customer with a copy of all policies and procedures in relation to its Security Programme.

10. Only authorised individuals shall be permitted by the Supplier to access the Customer Data under this Agreement. Access to Customer Data shall be revoked upon termination of such individuals' employment with or engagement by the Supplier.

PART B - INFORMATION SECURITY OBLIGATIONS

1. SECURITY REVIEWS

1.1 For the entire period that the Supplier processes, stores or otherwise has access to Customer Confidential Information, the Customer shall have the right to conduct an annual review of the Supplier's (and any sub-contractors) security program. The Supplier shall promptly (but in any event no later than thirty (30) days after receiving Customer's request to schedule and perform such review) schedule such a review for a date which is mutually agreeable. The Customer shall have access to the Supplier's Policies, procedures, and other relevant documentation and to the Supplier's Personnel as reasonably necessary to assist such reviews.

Within thirty (30) days following the completion of such a review, the Supplier shall provide a remediation plan to the Customer. Each issue shall be remediated by the Supplier in a timely manner, in line with a mutually agreed remediation schedule.

2. SPECIFIC SECURITY REQUIREMENTS

2.1 Security Policy

A comprehensive set of written security policies and procedures shall be maintained by the Supplier which include, at a minimum:

2.1.1 the Supplier's information security commitment;

2.1.2 information risk management; acceptable use of the Supplier's assets, including computing systems, networks, and messaging;

2.1.3 information classification, labelling, and handling, and such policies and procedures related to information handling must describe the permissible methods for information transmission, storage, and destruction and such methods must be no less protective than those set forth below and those in the Customer Supplier Information Protection Guidelines listed below;

2.2 The Supplier shall audit, review, and monitor its Information Security Program to confirm safeguards are appropriate to limit risks to Customer Confidential Information.

2.3 Asset and Information Management

2.3.1 All Customer Confidential Information that the Supplier processes or stores should be documented in an inventory by the Supplier;

2.3.2 All physical computing and software assets the Supplier uses in the performance of its activities under this Agreement should be documented in an inventory by the Supplier;

2.3.3 When handling, processing, and storing Customer Confidential Information the Supplier shall follow the Customer Supplier Information Protection Guidelines (as set out below).

2.4 Physical and Environmental Security

2.4.1 Access restrictions should be in place for the Supplier's area(s) where Customer Confidential Information is stored, accessed, or processed; Entry should be restricted solely to the Supplier's personnel authorized for such access;

2.4.2 Reasonable best practices for infrastructure systems, including fire extinguishing, HVAC, and power, emergency systems, and employee safety shall be maintained by the Supplier;

2.4.3 For the Supplier's area(s) where Customer Confidential Information is stored, accessed, or processed, physical entry controls commensurate with the sensitivity of the Customer Confidential Information shall be in place;

2.4.4 The Supplier's area(s) where Customer Confidential Information is handled, stored and/or processed shall be regularly monitored by the Supplier.

2.5 Employee-related Matters

2.5.1 Supplier personnel (including Contractors, where allowed by law) that have access to Customer Confidential Information, shall have criminal background checks performed by the Supplier, except to the extent limited or prohibited by applicable laws; Access to Customer Confidential Information must not be granted to individuals prior to the completion of such background checks and must not be granted to individuals who do not have a satisfactory background check.

2.5.2 The Supplier shall ensure its new personnel (including Contractors) are trained on the acceptable use and handling of the Supplier's confidential information and confidential information of other companies that has been entrusted to Supplier (for example Customer Confidential Information); Such training shall be reviewed by the Supplier annually and any necessary updates made;

2.5.3 Supplier personnel (including Contractors) shall be provided with security and data privacy education and training; Records shall be maintained to confirm which personnel have completed such education and the training should be reviewed by the Suppler annually and any necessary updates made;

2.5.4 The granting and revoking of access to the Supplier's information systems and services shall be managed by a formal user registration and de-registration procedure; An individual's access to Customer Confidential Information shall be removed by the Supplier as soon as possible but in any event no later than two (2) Working Days following termination of such individual.

2.6 Communications and Operations

2.6.1 The Supplier shall undertake regular backups sufficient to allow services to be restored to the Customer within the agreed upon recovery times (or, if no specific recovery times have been agreed to by the parties, within a commercially reasonable period); In addition, backup restore tests shall be performed at least once a quarter;

2.6.2 In line with the Customer Supplier Information Protection Guidelines set out in this document, the Supplier shall encrypt all backup media containing Customer Confidential Information;

2.6.3 Prior written consent of the Customer is required for the storage or replication of any Customer Confidential Information outside of Supplier's premises;

2.6.4 Prior written consent of the Customer is required for the transmission, transfer, or provision of any Customer Confidential Information to any third party, or provision of access to any Customer Confidential Information to any third party;

2.6.5 The Supplier shall, for any of the activities described in clauses 4.6.3 and 4.6.4 which are approved by Customer, hold an inventory of the third parties and/or locations outside of Supplier's premises that store or replicate any Customer Confidential Information, the third parties that receive or have access to Customer Confidential Information, the purpose for storing, replicating, providing or providing access to such Customer Confidential Information, the manner in which such Customer Confidential Information was transmitted or otherwise provided to such third party, the transmission and encryption/protection method or protocol (where applicable) used in transmitting or otherwise providing such Customer Confidential Information, a description of the Customer Confidential Information that was transmitted or otherwise provided to such third party, the name of the Customer employee that approved such arrangement and the date such approval was obtained;

2.6.6 Upon written request from the Customer, any or all Customer Confidential Information shall be promptly deleted or destroyed by the Supplier; Data destruction procedures that meet or exceed NIST SP 800-88 must be used;

2.6.7 When transmitting or transporting Customer Confidential Information the Supplier shall follow the Customer Supplier Information Protection Guidelines set out in a subsequent Schedule in this document, including those in relation to encryption;

2.6.8 All mobile devices on which any Customer Confidential Information is stored or that are used by Supplier's personnel to access any Customer Confidential Information should have hard drive encryption; Such encryption shall be in line with the Customer Supplier Information Protection Guidelines set out in a subsequent Schedule in this document;

2.6.9 The Supplier's servers and/or end user platforms that transmit, access, process or store Customer Confidential Information should have up to date malware detection and prevention in place;

2.6.10 A hardened Internet perimeter and secure infrastructure using firewalls, antivirus, anti-malware, intrusion detection systems, and other protection technologies should be maintained by the Supplier as is commercially reasonable;

2.6.11 All Supplier systems that transmit, access, process or store Customer Confidential Information should have regular patch management and system maintenance in place;

2.7 Access Control

2.7.1 Best practices for user authentication shall be enforced by the Supplier; If the Supplier uses passwords to authenticate individuals or automated processes accessing Customer Confidential Information, such passwords will comply with the current best practices for password usage, creation, storage, and protection (as set out in the Customer Supplier Information Protection Guidelines below).

2.7.2 User IDs must be unique to individuals and must not shared; Within 24 hours of a user's termination with the Supplier the User ID must be removed;

2.7.3 When accessing all IT environments, critical applications, and applications handling Customer Confidential and Customer Restricted Information Multi Factor Authentication must be enabled;

2.7.4 The Supplier shall assign access rights based upon the sensitivity of Customer Confidential Information, the individual's job requirements, and the individual's "need to know" for the specific Customer Confidential Information;

2.7.5 The Supplier shall carry out access rights reviews at least annually for the Supplier's personnel (including Contractors) to ensure need-to-know restrictions are kept up to date;

2.7.6 Reports of user entry into the Supplier's facilities housing Customer Confidential Information should be regularly reviewed by the Supplier;

2.7.7 The Supplier shall not leave Customer Confidential Information unattended on desktops, printers or elsewhere in an unsecure manner in the Supplier's facilities.

2.8 Application Development; Vulnerability Scans and Penetration Tests

2.8.1 A secure development methodology incorporating security throughout the development lifecycle should be employed by the Supplier;

2.8.2 Secure coding standards must be developed and enforced by the Supplier;

2.8.3 All internet-facing applications and any software developed by the Supplier (or a Contractor) for delivery to the Customer must have secure code reviews completed using automated scanning tools before deployment to production;

2.8.4 All externally-facing applications that receive, access, process or store Customer Confidential Information must be scanned for vulnerability at least once a month; The Supplier should confirm in writing, if requested by the Customer, that the Supplier has successfully performed such vulnerability scans and shall remediate vulnerabilities classified as "critical" or "high" within thirty (30) days for high severity vulnerabilities or, if such issue(s) cannot be corrected within such thirty (30) day period, within a period of time mutually agreed to by Supplier and Customer;

2.8.5 All of the Supplier's externally-facing applications that receive, access, process or store Customer Restricted Information should have penetration tests conducted by an external third-party security testing company approved by the Customer at least annually; The Supplier shall, where requested by the Customer, confirm in writing that the Supplier has successfully performed such penetration tests; All material issues (those classified as "critical", "important", "high", or "medium" discovered in the course of such penetration tests conducted by or on behalf of Supplier) shall be corrected by the Supplier within thirty (30) days or, if such issue(s) cannot be corrected within such thirty (30) day period, within a period of time mutually agreed to by the Supplier and the Customer.

2.9 Contractors

2.9.1 The Supplier shall take reasonable steps to select and maintain Contractors that are capable of maintaining security measures to protect Customer Confidential Information in accordance with applicable laws and regulations and in a manner no less protective than the requirements set out in this Agreement, including this Schedule; A written contract should be put in place by the Supplier for each such Contractor, which requires the Contractor, by contract, to implement and maintain such security measures;

2.9.2 Prior written consent of the Customer is required to provide any Contractor, or allow any Contractor to access, process, store, view or otherwise interact with, any Customer Confidential Information;

2.9.3 The Supplier shall be responsible to Customer for all acts and omissions of any Contractor, including any failure by a Contractor to comply with the provisions of this Agreement, including this Schedule;

2.9.4 Regular reviews of each Contractor, including a review of the Contractor's information security policies and practices, shall be carried out by the Supplier.

3. INFORMATION SECURITY INCIDENT MANAGEMENT

3.1 An information security incident response process shall be established, tested, and maintained by the Supplier, including processes for evidence preservation, informing, and working with law enforcement agencies, government agencies and similar parties as appropriate, and performing forensic analyses;

3.2 Information security breaches involving Customer Confidential Information, including any actual or suspected unauthorized access to Customer Confidential Information or a security incident at or involving a Contractor's systems, hardware, equipment, devices or premises computers or otherwise involving a Contractor's personnel shall be notified to the Customer by the Supplier in writing; Notification of any such incident should be provided by the Supplier as soon as possible, but in any event, no later than twenty-four (24) hours following the date the Supplier first becomes aware of such incident. The Supplier should provide regular updates to the Customer regarding the investigation and mitigation of such an event following the initial notification. The Customer or its designees shall be allowed by the Supplier to take part in all aspects of the investigation. All costs incurred by any party in connection with such incidents, are the responsibility of the Supplier, including but not limited to, notification of affected data subjects, forensic investigations, credit monitoring for data subjects and other remedial and legal efforts;

3.3 The Supplier shall provide the Customer, for each such incident, with a final written notification no later than ten (10) days following the Supplier's closure of such incident, that includes detailed information regarding the root cause of such incident, actions taken, and plans to prevent a similar event from occurring in the future.

4. BUSINESS CONTINUITY MANAGEMENT

4.1 A comprehensive business continuity plan ("BCP") that covers the reinstatement of both technology and business operations in the event of an unplanned event shall be implemented and maintained by the Supplier;

4.2 The Supplier shall test or review its BCP at least once a year in a manner it considers suitable, exercising its sole and absolute judgment;

4.3 The Customer shall be informed by the Supplier of its plans to maintain service levels in both normal conditions and during disruptive events.

verian

5. COMPLIANCE

5.1 The Customer Supplier Information Protection Guidelines set out in a subsequent Schedule in this document shall be abided to by the Supplier;

5.2 Mutually agreed policies and practices for records retention and data destruction applicable to the Customer Confidential Information and any other information produced during or otherwise related to Supplier's activities under this Agreement shall be implemented and maintained by the Supplier;

5.3 A code of ethics should be established by the Supplier and employees shall be required to review and acknowledge it once a year (except if and to the extent prohibited by law).

6. FOLLOW-UP RISK MANAGEMENT ACTIONS

If a security review of the Supplier and/or one or more of its facilities (or those of its Contractors, as applicable) conducted by the Customer has identified one or more items of concern, the Supplier shall:

6.1 cooperate with the Customer to develop, without delay, a mutually agreeable risk management plan to remediate such items of concern, and

6.2 implement the actions set out in the risk management plan no later than the corresponding date specified in such risk management plan.

7. IDENTITY THEFT

In relation to any Personal Information the Supplier processes, handles or has access to, the Supplier shall notify the Customer without delay if the Supplier's employees become aware of any potential identity theft related to the individual(s) to which such Personal Information relates during the Supplier's activities under this Agreement.

8. UPDATES

This Information Security Addendum may be updated by the Customer at any time upon thirty (30) days prior written notice to Supplier. If the Supplier feels it cannot comply with such updates, the Customer should be notified in writing within such thirty (30) day period setting out the specific items the Supplier cannot meet. The Customer, in such event, reserves the right to terminate any or all services or projects with the Supplier without liability or penalty on account of such termination.

verian

PART C – CUSTOMER SUPPLIER INFORMATION PROTECTION GUIDELINES

1. CUSTOMER INFORMATION CLASSIFICATION AND HANDLING MATRIX

Without limiting the Supplier's obligations as specified in this Agreement, including this Schedule, the following table summarises specific requirements for transmitting (or transferring), storing or destroying Customer Confidential Information, including Customer Restricted Information:

Information Classification	Examples	Transmission	Storage	Destruction
Customer Confidential Information other than Customer Restricted Information	Supplier briefing documents; Internal business data e.g. strategy Audit reports; Pre-release marketing information; Customer proprietary software; Business continuity infrastructure plans	Electronic: Encrypt when transmitted over public networks or transferred outside of Supplier's premises on portable media or devices or other electronic media; Print: Send via courier (including overnight delivery service) or registered mail with tracking number.	Limit access to authorised personnel only; perform quarterly access rights reviews. Encryption when in storage preferred.	Electronic: Use NIST SP 800-88 or equivalent procedures. Print: Shred using a cross-shred paper shredder, complaint to ISO/IEC 21964 (DIN 66399) or disposal via a certified destruction provider.
Customer Restricted Information	Personal Information (including name, email address, telephone number, postal address, ID, or account numbers) Personal financial information Personal health information	Same as above	Limit access to authorised personnel only; perform quarterly access rights reviews. Encryption in storage required.	Same as above

2. ENCRYPTION

The Customer's current preferred encryption algorithms and current additional acceptable encryption algorithms are specified in the table below. The Supplier shall use one of the preferred encryption algorithms when encrypting Customer Confidential Information unless it is not reasonably feasible to do so, in which case the Supplier shall use one of the additional acceptable encryption algorithms when encrypting Customer Confidential Information.

Preferred Encryption Algorithms		
Purpose	**Algorithms**	**Minimum Key Length (Bits)**
Key Exchange	RSA	2048 preferred, if not possible then 1024
Data Protection	AES in CBC mode	256 preferred, if not possible then 128
Hash	SHA-256	N/A
HMAC	HMAC SHA-256	256
Digital Signature	RSA with SHA-256 DSA with SHA-256	2048 preferred, if not possible then 1024

Additional Acceptable Encryption Algorithms		
Purpose	**Algorithms**	**Minimum Key Length (Bits)**
Data Protection	AES in GCM mode	1024 if possible, else 248
Hash	SHA-256 preferred, if not possible then SHA-2.	N/A
HMAC	HMAC SHA-256 preferred, if not possible then SHA-2 SHA-1 & MD5 should never be used unless an exception for technology is needed.	256 preferred, else 128
Digital Signature	ECC with SHA-256, if not possible then SHA-2 RSA with SHA-256 preferred, if not possible then SHA-2, DSA with SHA-256 preferred, if not possible then SHA-2	160 min 20148 preferred, if not possible then 1024

Password-based Authentication Guidelines.

The Supplier shall ensure that all passwords administered or controlled by the Supplier (or a Contractor) meet the following or NIST SP 800-63B guidelines.

Area	Guideline
Password complexity	Two of the four-character types (upper, lower, digits, special), should not be easily associated with an individual or process, not found in a dictionary and not represent a pattern. It is strongly recommended that passwords contain three of the four-character types.
Maximum password lifetime	No expiry but passwords shall force a change if there is evidence of compromise.
Minimum password history	One day.
Protection in transit	Mandatory. Passwords must be encrypted in transit.
Protection in storage	Mandatory. Passwords must be hashed using an approved hash algorithm (see table above).