

Supplier Information Security Obligations

1. INTRODUCTION

This document sets out Verian's minimum contractual information security obligations for Suppliers that store, process or have access to Verian information as part of delivering services.

These obligations form one component of Verian's wider supplier risk and assurance framework, which is designed to apply appropriate and proportionate controls across the full supplier lifecycle.

Supplier security is assessed prior to contract award through Verian's supplier due diligence and assurance processes, which may include risk-based questionnaires, independent certifications, remediation plans, or other evidence proportionate to the nature of the services and information involved.

The requirements in this document apply in addition to any selection-stage assurance activities and are intended to ensure that agreed security standards are maintained throughout the term of the engagement, including through ongoing monitoring and review where appropriate.

Not all provisions in this document will be relevant to every Supplier or Engagement. Applicability is determined based on the risk, scale and sensitivity of the services provided and the information involved, as agreed with Verian.

Compliance with these obligations is supported by Verian's Information Security Management System.

Supplier Information Security Obligations

2. TERMINOLOGY

The terms below (whether used with initial upper case or in all lower case) shall have the corresponding meaning as described. The Oxford English Dictionary shall be the authoritative reference for all other definitions.

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

Supplier: the entity specified in the PO.

Customer Information: Any information, data or materials provided to the Supplier by, or on behalf of, the Customer, or generated, collected or processed by the Supplier in connection with the services, including information relating to the Customer's business, operations, systems, personnel, clients or research activities.

Customer Information may exist in any form, including electronic, physical, visual or verbal.

Customer Restricted Information: Customer Information that is classified by Verian as Restricted under Verian's Data Classification and Handling Policy, being highly sensitive information, including personal data, that requires the highest level of protection and is restricted to authorised individuals only.

For the purposes of this document, references to Customer Information include Customer Restricted Information unless otherwise stated.

Good security practice: security practices as detailed and recommended by the UK National Cyber Security Centre (NCSC), or equivalent recognised national cybersecurity authority.

Information security incident: Adverse event likely to affect the confidentiality, integrity or availability of Customer Information.

Supplier Information Security Obligations

PART A - Overview

1. The Supplier shall implement risk-appropriate physical, technical and organisational security controls to prevent unauthorised access to systems, devices and information used in connection with this Agreement, in line with good security practice.
2. 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 Information or the systems put in place between the parties to transfer and/or provide access to Customer Information;
3. 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 Information 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.

Supplier Information Security Obligations

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 Information, the Customer shall have the right to conduct an annual review of the Supplier's (and any sub-contractors) security programme against the obligations set out in this and related documents.

1.2 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.

1.3 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.

1.4 Following a review, the Customer will provide a list of findings to the Supplier, detailing issues and matters to be addressed.

1.5 Within thirty (30) days following the completion of such a review, the Supplier shall provide a remediation plan to the Customer.

1.6 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

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

1. the Supplier's information security commitments;
2. information risk management;
3. acceptable use of the Supplier's assets, including computing systems, networks, and messaging;
4. information classification, labelling, and handling;
5. records retention

2.2 Audit and Review

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

2.3 Asset and Information Management

2.3.1 All Customer Information that the Supplier processes or stores shall 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 shall be documented in an inventory by the Supplier.

2.4 Password and Authentication Controls

2.4.1 Where passwords are used to authenticate access to systems handling Customer Information, the Supplier shall implement controls consistent with current NCSC guidance on password and authentication security, or equivalent industry best practice.

Supplier Information Security Obligations

2.4.1 This includes, but is not limited to:

- protection of credentials in transit and at rest
- resistance to brute force and credential stuffing attacks
- use of multi factor authentication where appropriate
- secure storage and handling of authentication secrets

2.5 Encryption and cryptography

2.5.1 The Supplier shall protect Customer Information and Customer Restricted Information (including that stored in back-ups) using strong, industry standard cryptographic controls, appropriate to the sensitivity of the information and the risk of the processing activity.

2.5.2 Cryptographic controls shall follow current guidance published by the UK National Cyber Security Centre (NCSC), or an equivalent recognised national authority, including guidance on:

- encryption of data in transit
- encryption of data at rest
- key management
- cryptographic algorithm and protocol selection

2.5.3 Where cryptographic standards evolve, the Supplier shall ensure that controls are kept up to date in line with such guidance.

2.6 Physical and Environmental Security

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

2.6.2 Reasonable best practices for infrastructure systems, including fire control, HVAC, and power, emergency systems, and employee safety shall be maintained by the Supplier.

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

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

2.7 Employee-related Matters

2.7.1 Supplier personnel (including Contractors, where allowed by law) that have access to Customer Information, shall have criminal background checks performed by the Supplier, except to the extent limited or prohibited by applicable laws.

2.7.2 Access to Customer Information shall not be granted to individuals prior to the completion of such background checks and shall not be granted to individuals who do not have a satisfactory background check.

2.7.3 Supplier personnel (including Contractors) with access to Customer Information shall receive appropriate information security, data protection and acceptable use training, commensurate with their role, at onboarding and at least annually thereafter. Training shall be reviewed periodically and records of completion shall be maintained.

Supplier Information Security Obligations

2.7.4 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.

2.7.5 An individual's access to Customer 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.

2.8 Communications and Operations

2.8.1 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); backup restore tests shall be performed at least once a quarter.

2.8.2 Prior written consent of the Customer is required for the storage or replication of any Customer Information outside of Supplier's premises.

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

2.8.4 As part of its information asset and supplier inventories, 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 Information
- the third parties that receive or have access to Customer Information

2.8.5 Each record shall specify:

- the purpose for storing, replicating, providing or providing access to such Customer Information
- the manner in which such Customer 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 Information
- a description of the Customer Information that was transmitted or otherwise provided to such third party
- the name of the Customer employee that approved such arrangement
- the date such approval was obtained.

2.8.6 Upon written request from the Customer, any or all Customer Information shall be promptly deleted or destroyed by the Supplier as specified in Part C.

2.8.7 When transmitting or transporting Customer Information, the Supplier shall follow the handling instructions in Part C.

2.8.8 All mobile devices on which any Customer Information is stored, or that are used by Supplier's personnel to access any Customer Information, shall have hard drive encryption in place.

2.8.9 The Supplier's servers and other devices that store, process or transmit Customer

Supplier Information Security Obligations

Information shall have up to date malware detection and prevention in place.

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

2.8.11 All Supplier systems that transmit, access, process or store Customer Information shall have regular system maintenance in place.

2.9 Access Control

2.9.1 Best practices for user authentication shall be enforced by the Supplier; if the Supplier uses passwords to authenticate individuals or automated processes accessing Customer Information, such passwords will comply with current good practice for password usage, creation, storage, and protection.

2.9.2 User IDs shall be unique to individuals and shall not be shared. Within 24 hours of a user's termination with the Supplier, the User ID shall be removed.

2.9.3 When accessing all IT environments, critical applications, and applications handling Customer Information, Multi Factor Authentication shall be in place and mandated for all users.

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

2.9.5 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.

2.9.6 Reports of user entry into the Supplier's facilities housing Customer Information shall be regularly reviewed by the Supplier.

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

2.10 Application Development

2.10.1 A secure development methodology incorporating security throughout the development lifecycle shall be employed by the Supplier.

2.10.2 Secure coding standards shall be developed and enforced by the Supplier.

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

2.11 Vulnerability Management

2.11.1 All software, operating systems, and other IT elements that store, process or transmit Customer Information shall be monitored for vulnerabilities, and any identified vulnerabilities shall be remediated in line with the specifications in the current Cyber Essentials standard.

2.11.2 All of the Supplier's external-facing applications that receive, access, process or store Customer Restricted Information shall have penetration tests conducted by an independent entity certified to CHECK standard, at least annually.

2.11.3 The Supplier shall, where requested by the Customer, confirm in writing that the Supplier has successfully performed such penetration tests.

Supplier Information Security Obligations

2.11.4 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 by the Supplier and the Customer.

2.12 Contractors

2.12.1 The Supplier shall take reasonable steps to select and maintain Contractors that are capable of maintaining security measures to protect Customer 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.

2.12.2 A written contract shall be put in place by the Supplier for each such Contractor, which requires the Contractor, by contract, to implement and maintain such security measures;

2.12.3 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 Information.

2.12.4 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.

2.12.5 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 incidents shall be notified to the Customer by the Supplier in writing.

3.3 Notification of an information security incident shall 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.

3.4 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.

3.5 The Supplier shall provide regular updates to the Customer regarding the investigation and mitigation of information security incidents following the initial notification.

3.6 The Customer or its designees shall be allowed by the Supplier to take part in all aspects of the investigation.

3.7 All costs incurred by any party in connection with information security 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.

3.8 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

Supplier Information Security Obligations

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.

5. COMPLIANCE

5.2 A code of ethics shall 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

6.1 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:

- cooperate with the Customer to develop, without delay, a mutually agreeable risk management plan to remediate such items of concern, and
- implement the actions set out in the risk management plan no later than the corresponding date specified in such risk management plan.

8. UPDATES

8.1 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 shall 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.

Supplier Information Security Obligations

Part C - INFORMATION CLASSIFICATION AND HANDLING

The requirements in this section form an integral and mandatory part of the Supplier's information security obligations under this Agreement.

The following table provides requirements for transmitting (or transferring), storing and destroying Customer Information:

Information Classification	Examples	Transmission	Storage	Destruction
Customer 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.	Perform quarterly access rights reviews. Encryption preferred.	Electronic: Use NIST SP 800-88 or equivalent procedures. Print: Shred using a cross-shred paper shredder, compliant 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	Perform quarterly access rights reviews. Encryption required.	Same as above

Supplier Information Security Obligations

Document Owner	Verian Group Information Security
Senior Owner	Global CISO
Approved by	Global CISO
Issue Date	19/03/2024
Last Reviewed	14/04/2026
Review Cycle	Annual, or upon material change.