Minimum Security Requirements for Suppliers

These may be used as technical and organisational security measures to be implemented by the Supplier in accordance with Standard Contractual Clauses 4(d) and 5(c) at Suppliers risk:

The Supplier (and its sub-processors) must implement the following technical and organisational measures designed to prevent accidental or unlawful destruction or accidental loss, alteration unauthorised disclosure or access, and to maintain principles of confidentiality, integrity, and availability:

Security Assurance

Client reserves the right to audit the Supplier, either itself or through an authorized representative, using an ISO27001 aligned; Standard Information Gathering (SIG) aligned; or bespoke format cybersecurity assessment relating to the services provided. Unless Client reasonably believes that a security incident may have occurred, Client must have the right to perform a cybersecurity assessment once per calendar year.

Client shall provide Supplier with at least thirty (30) days advance notice of a cybersecurity assessment. Supplier must provide all assistance and resources reasonably required to perform a cybersecurity assessment at no expense to Client. Supplier must provide available external security audit reports and scoping documents (e.g., ISO27001, SOC2) upon request.

Supplier must remedy any identified material cybersecurity deficiencies in a timely manner, with critical issues remediated within 30 days, and all other material issues remediated within 90 calendar days unless agreed otherwise in writing.

Security Governance

G.1 The Supplier’s collective security measures (e.g., Information Security Policy) must comply with applicable privacy and data security laws.

G.2 The Supplier must document the Information Security Policy (program and/or procedures) in written form for the handling of personal or sensitive data and must make those documents available to Client for review upon Clients’ request.

G.3 The Supplier must maintain its Information Security Policy at least annually to improve the security of the Information Security Program, but in no event render it less comprehensive, secure, or robust.

G.4 Where the Supplier provides or uses 3rd party technology systems (or parts thereof) material to the delivery of services, they must be independently certified to an internationally recognised security standard (e.g., ISO/IEC 27000 series, NIST Cybersecurity Framework, or CIS Critical Security Controls).

Security Management

M.1 Supplier must ensure that the security measures implemented in accordance with this Annex are regularly tested, assessed, and evaluated in terms of their effectiveness in securing relevant Personal Data through regular management.

M.2 Where applicable for software development, the Supplier (or their suppliers) will perform application security analysis and testing according to the verification requirements of an agreed-upon standard (e.g., OWASP Application Security Verification Standard). The Supplier must document verification findings according to the reporting requirements of the standard and provide the verification findings to Client on request.

M.3 For web or hosted applications used in provision of service, Supplier must ensure network and application penetration testing and vulnerability assessments are undertaken at least annually by certified external third parties (e.g., CREST or CHECK certified) for any web or hosted applications.

M.4 The Supplier must implement a security awareness, anti-phishing, and data compliance training at least annually to ensure that all data handlers and supporting staff have appropriate knowledge of procedures (including Art. 29 obligations) to ensure compliance and minimise data security risks. All data handlers must be subject to confidentiality agreement.

Business Continuity Management

B.1 Supplier must establish a Business Continuity Management programme that supports our regulatory, statutory, and contractual requirements, including Art. 32 1(c).

B.2 Suppliers’ offices, services lines and functions are included within the business continuity management programme and are required to have in place a business continuity plan. The business continuity plans, and disaster recovery plans must be developed and maintained by assigned owners across business and information technology functions and are regularly updated at least annually to reflect any change of circumstances.

B.3 Where the Supplier provides technology systems, annual testing and reviews must be carried out on all plans in line with international best practice (e.g., ISO22301, or equivalent)

Security Incident Management

I.1 The Supplier must create and maintain a global risk-based processes to respond to information security incidents, unusual or suspicious events and breaches of policies.

I.2 The Supplier must provide commercially reasonable assistance to Client in fulfilling any legal notification obligations that arise in connection with such a Data Breach in a timely manner (e.g., 5 days).

I.3 Supplier must ensure that all systems have sufficient level of logging and monitoring to prevent, detect and respond to security incidents (e.g., 24x7 Security Operations Centre).

I.4 The Supplier must implement information security incident management processes designed to contain and control the incident, reduce any potential impact to the business, identify and investigate the root cause and implement corrective actions to reduce the risk of recurrence.

I.5 Breaches of all security and suspected weaknesses are formally reported, investigated, documented, and resolved, and reported to senior management.

I.6 The Supplier must notify Client in writing at informationsecurity@controlrisks.com of any suspected or confirmed Data Breach (defined as a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so) involving Client Information within forty-eight (48) hours after the Supplier discovers or is notified of such a Data Breach.

I.7 Such notice must include at least, to the extent known by the Supplier: (a) the nature and duration of the Data Breach; (b) the types and volume of Information impacted by the Data Breach, including the identities of any individuals whose Personal Information was affected; (c) steps Supplier has taken and will take to investigate, remediate, and mitigate the effects of the Data Breach; and (d) any other information Client might reasonably request regarding the incident.

Data Management

D.1 The Supplier must define and publish a Data Classification & Data Retention, Archiving and Destruction Policy (DRAD) Policy with regards to the data it stores, process or transmits, or that is in its custody or under its control. The policy obligations must include how long the Supplier may retain data (typically less than 3 years), and when and how it can destroy data to meet relevant laws, regulations and/or contracts.

D.1 System backups must be performed regularly (e.g., daily) such that the system can be restored within target times, and in any case no less than 48 hours, without loss of data or data integrity.

D.2 Backup media must be stored separately to the primary system to prevent corruption or compromise and must be tested at least annually.

D.3 Upon expiration or termination of the Agreement, or at any time upon request by Client and at no cost to Client, Supplier will return to Client and/or destroy all Personal Data held in any form or medium whatsoever, collected or received from or on behalf of Client. Supplier will promptly, and in any case within 14 days, send Client a written acknowledgment that all Personal Data has been returned and/or destroyed.

D.4 Where the Supplier provides technology systems, they must ensure that data is logically or physically segregated from other client or customer data to minimise the risks of data leakage. Test data must use pseudonymisation where applicable and be segregated from production systems.

Logical & Role Based Access Control

L.1 Supplier must ensure information and systems are only available to authorised employees with a justified business need. All access is based on the employee's role and there is a formal approval process prior to access being granted.

L.2 Where possible, Supplier must implement 'least privilege' approach to system access (e.g., role-based access). This ensures that authorised employees have minimal access to Supplier data, applications, systems, networks, and devices.

L.3 Supplier must ensure employees are assigned unique user IDs and password management must be automatically enforced using industry standards (e.g., Centre for Internet Security).

L.4 Supplier must ensure the use of privileged accounts is strictly controlled and their usage limited to system administration and maintenance activities only. For clarity, privileged accounts must not be used for general or non-privileged activities.

L.5 Supplier must ensure remote access to the Supplier network is only permitted for pre-authorised employees, contractors or suppliers using a Supplier' managed asset with multi-factor authentication (e.g., encrypted VPN solution).

Communications and Operations Security

CO.1 Supplier must ensure its IT systems are configured to international technical security standards which include applicable controls such as system hardening, encryption, anti-virus and data loss prevention, regular patching (at least monthly), security updates and adequate monitoring.

CO.2 Wireless network must utilise only secure wireless security standards (e.g., WPA2, EAP-TLS), with any visitor or guest Wi-Fi networks segregated from primary network.

CO.3 Appropriate to the size of the organisation, Supplier must implement a defence-in-depth approach to protect its information and IT systems that includes the formalisation of processes and procedures to support key activities such as back-up, change management, release management, business continuity, disaster recovery and incident management.

CO.4 Where applicable for web or hosted applications, using layers of firewalls, secure segregation of different networks, connections, and systems. Supplier must ensure it has a disaster tolerant network and system architecture design across all its global data (and call centres where applicable) with 24/7 monitoring.

Cryptography and Pseudonymisation

CP.1 Supplier must ensure all applications and systems use the latest internationally recognised standards of encryption algorithms (e.g., FIPS 401-2) and supporting processes that conform to industry standards for encryption and key management.

CP.2 Supplier must ensure that:

- all portable devices (e.g., laptops, USB) have full disk encryption.
- back-end mass storage (databases, server files) is encrypted-at-rest.
- backups are encrypted.
- exchanges of Personal Data across untrusted networks are encrypted-in-transit (e.g., TLS, IPSEC).
- all Personal Data is encrypted at rest.
- test systems must utilise pseudonymisation of personal data in accordance with Art. 32 1(a).

Physical and Environmental Security

P.1 Supplier must ensure it uses data processing facilities (e.g., datacentres, call centres, file storage) which are ISO27001 and/or SOC II Type 2 certified. These buildings must provide protection against unauthorised physical access used for processing Personal Data. These include physical and electronic access control systems, manned reception desks, visitor booking systems, CCTV, and security lighting. Datacentres should be rated Tier 3+, which provides a high level of redundancy, physical security, and environmental controls. Using certified cloud providers (e.g., Microsoft, Google, AWS) will typically provide these controls as standard.

P.2 Documents (defined as any piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record) must be stored securely and be disposed of in accordance with an approved shredder (e.g., DIN 66399 P4 standard or higher). Any documents with personal data destroyed by a 3rd party must be evidenced by a certificate of destruction.

P.3 Hardware (defined as any electronic equipment that stores, processes, or transmits Client data) must be always stored securely, and then securely wiped to US Department of Defence 5220-22M Manual or NIST 800-88 Clear or Purge Standard prior to a) being sent to a 3rd party for repair b) re-use in another system; and/or c) permanent disposal (in compliance with Waste Electrical and Electronic Equipment (WEEE) directive as applicable). A certificate of destruction must be maintained for at least 12 months.

Control Risks

Minimum Security Requirements for Subcontractors

These may be used as the technical and organisational security measures to be implemented by the Subcontractors in accordance with Standard Contractual Clauses 4(d) and 5(c) at Subcontractors risk:

The Subcontractor (and its sub-processors) must implement the following technical and organisational measures designed to prevent accidental or unlawful destruction or accidental loss, alteration unauthorised disclosure or access, and to maintain principles of confidentiality, integrity, and availability:

Security Assurance

Client reserves the right to audit the Subcontractor, either itself or through an authorized representative using a questionnaire or site visit.

Subcontractor must provide all assistance and resources reasonably required to perform a cybersecurity assessment at no expense to Client.

Subcontractor must remedy any identified material deficiencies in a timely manner, with critical issues remediated within 30 days, and all other material issues remediated within 90 calendar days unless agreed otherwise in writing.

Unless Client reasonably believes that a security incident may have occurred, Client will have the right to perform a cybersecurity assessment once per calendar year.

Security Governance

Subcontractor must comply with applicable privacy and data security laws. A security policy is strongly recommended.

Subcontractor must document in written form the handling of personal or sensitive data from Client and must make those documents available to Client for review upon Clients' request.

Subcontractor should review data handling procedures at least annually to improve the security of data handling, and any changes must not render the process less comprehensive, secure, or robust.

Security Management

Subcontractor must ensure that the data security measures implemented are regularly evaluated (at least annually) in terms of their effectiveness in securing relevant Personal Data.

We strongly recommend that Subcontractor use certified cloud services (e.g., Office365, GoogleApps, AWS) which are ISO27001, NIST and/or SOC II Type 2 certified.

Subcontractor must implement a basic security awareness/anti-phishing training. Free training modules are available at UK's National Cyber Security Centre: https://www.ncsc.gov.uk/training/cyber-security-for-small-organisations-scorm-v2/scormcontent/index.html

Data compliance training should also be completed at least annually to ensure that all data handlers and supporting staff have appropriate knowledge of procedures (including Art. 29 obligations) to ensure compliance and data security.

All data handlers must be subject to confidentiality agreement.

Business Continuity

Subcontractor must establish a plan that supports the regulatory, statutory, and contractual requirements for their business, including Art. 32 1(c), for business continuity and disaster recovery (e.g., loss of premises, loss or malfunction of hardware and/or loss of system access).

Security Incident Management

Subcontractor must respond to security incidents in a timely manner to contain and control the impact and achieve a full recovery, especially unusual or suspicious events and breaches of policies.

Subcontractor must ensure that all systems have sufficient level of logging and monitoring to prevent, detect and respond to security incidents. This is usually provided by your cloud or security software provider, and you should seek professional assistance where required.

Subcontractor must notify Client in writing at informationsecurity@controlrisks.com of any suspected or confirmed Data Breach (defined as a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so) involving Client Information within forty-eight (48) hours after the Subcontractor discovers or is notified of such a Data Breach.

November 2022

Such notice must include at least, to the extent known by the Subcontractor: (a) the nature and duration of the Data Breach; (b) the types and volume of Information impacted by the Data Breach, including the identities of any individuals whose Personal Information was affected; (c) steps Subcontractor has taken and will take to investigate, remediate, and mitigate the effects of the Data Breach; and (d) any other information Client might reasonably request regarding the incident.

Subcontractor must provide commercially reasonable assistance to Client in fulfilling any legal notification obligations that arise in connection with such a Data Breach in a timely manner (typically 5 days).

Data Management

Subcontractor must define how long they will retain data (typically 3 years), and when and how it will destroy data to meet relevant laws, regulations and/or contracts.

System backups must be performed regularly (e.g., daily) such that the system can be restored within target times, and in any case no less than 48 hours, without loss of data or data integrity. Cloud providers may do this automatically.

Encrypted backup media, where applicable, must be stored separately to the primary system to prevent physical damage, corruption or compromise and must be tested at least annually.

Upon expiration or termination of the Agreement, or at any time upon request by Client and at no cost to Client, Subcontractor will return to Client and/or destroy all Personal Data held in any form or medium whatsoever, collected or received from or on behalf of Client. Subcontractor will promptly, and in any case within 14 days, send Client a written acknowledgment that all Personal Data has been returned and/or destroyed.

Logical & Role Based Access Control

Subcontractor must ensure information and systems are only available to authorised employees with a justified business need. All access should be based on the minimum needs for an employee's or contractor's role.

Subcontractor must ensure employees are assigned individual user IDs, where password management is automatically enforced to effective security standards (e.g., 14-character password length, account lockout after 5 failed attempts).

Subcontractor must ensure the use of privileged / administrator accounts is restricted, and their usage limited to system administration activities only. For clarity, we strongly recommend that privileged accounts should not be used for general day-to-day activities to minimise risks from malware, and a separate user account should be created for everyday use.

Subcontractor must ensure remote access to their network or systems is only permitted for pre-authorised employees, contractors or suppliers using 'authorisation on connection' for occasional access or multi-factor authentication for longer term access.
Communications and Operations Security

Subcontractor must ensure its IT systems are configured to an acceptable technical security standard which should include security controls such as system hardening, encryption, anti-virus, and backup/data loss prevention. We strongly recommend your network and computer systems are setup securely by an IT professional.

We strongly recommend that you apply regular security and system updates at least monthly, and/or utilise manufacturer's "auto-update' feature where possible.

Subcontractor's wireless network must utilise only secure wireless security standards (e.g., WPA2), with any visitor or guest Wi-Fi networks must be securely segregated from the primary network.

Cryptography and Pseudonymisation

Subcontractor must ensure all applications and systems use good quality encryption. The US government publishes approved encryption standards under NIST FIPS 140 standards.

Subcontractor must ensure that:

- all portable devices (e.g., laptops, USB) have full disk encryption.
- back-end mass storage (backup devices, databases, server files) must be encrypted-at-rest.
- backup files and media must be encrypted.
- all Personal Data is encrypted at rest (e.g., databases).
- test systems, if applicable, must utilise pseudonymisation of personal data in accordance with Art. 32 1(a).

Exchanges of Personal Data across untrusted networks (e.g., internet, public Wi-Fi) must be encrypted-in-transit (e.g., https) or use a secure VPN tunnel.

Email is not secure by default and is therefore not suitable for transferring sensitive information or high volumes of personal information. All attachments must be securely encrypted. We strongly recommend that you send the decryption instructions via another method (e.g., SMS, phone call)

Physical and Environmental Security

We strongly recommend that Subcontractors use certified data or cloud processing facilities (e.g., Office365, GoogleApps, AWS) which are ISO27001 and/or SOC II Type 2 certified.

Subcontractor buildings used for processing Personal Data must provide protection against unauthorised physical access. These include appropriate physical (e.g., locks) and/or electronic access control systems.

Subcontractor documents (defined as any piece of written, printed, or electronic matter that provides information or evidence or that serves as an official record) containing Client data must be stored securely and be disposed of in accordance with an approved shredder (e.g., DIN 66399 P4 standard or higher). Any documents with personal data destroyed by a 3rd party must be evidenced by a certificate of destruction.

Hardware (defined as any electronic equipment that stores, processes, or transmits data) managing Client data must be always stored securely. We strongly recommend that all data is securely wiped by a professional service prior to a) being sent to a 3rd party for repair b) re-use in another system; and/or c) permanent disposal or sale.

We strongly recommend that any Subcontractor hardware disposal complies with Waste Electrical and Electronic Equipment (WEEE) directive, or equivalent, where applicable. A certificate of destruction must be maintained for at least 12 months.

Further Guidance Notes for Subcontractors

This quick guide is intended for sole traders or smaller entities supplying non-technology related services.

Security Governance

- A range of Information Security Policy templates are available from SANS website: https://www.sans.org/information-security-policy

- Here is a sample privacy notice for your website: https://ico.org.uk/for-organisations/make-your-own-privacy-notice/

Security Management

- Free training and awareness tools are available from National Cyber Security Centre at https://www.ncsc.gov.uk/.

Business Continuity Planning

- You can find a free guide from the UK's Federation of Small Business (FSB) here: https://www.fsb.org.uk/resources-page/how-to-create-a-business-continuity-plan.html

- A free Data Recovery Plan Policy is available here: https://www.sans.org/information-security-policy/

- The key requirement is to ensure is that critical data is backed up securely and can be restored on request. Cloud solutions like Office 365 (using OneDrive) may do this automatically where configured.

Security Incident Management

- A sample Data Breach Response Policy template is available here: https://www.sans.org/information-security-policy

Data Management

- Data Retention, Archiving and Destruction Policy (DRAD) Policy can be as simple as stating when personal or sensitive data will be deleted (e.g., 3 years)

- System backups from cloud solutions like Office 365 (using OneDrive) may happen automatically.

- Backup media for cloud solutions like Office 365 (using OneDrive) may not be required.

- Data on backup devices and mobile devices must be encrypted.

Logical Access Control

- Don't use generic account names like "Administrator" or "User1", create a separate account for each user access and keep administrator accounts for technical changes only.

- Enforce/use password standards of at least 14 characters long.

- If 3rd party access is required, then this should be only enabled when required over a secure connection.

Communications & Operation Security

- Desktops and laptops should have endpoint security software to protect against malware infections, provide whole-disk encryption and alert for system updates.

- Wireless networks should be configured to use WPA2 Wi-Fi security or better.

Cryptography & Pseudonymisation

- Data on mobile devices such as laptops and USB keys must be encrypted.

- Data should be transferred securely; email is not normally encrypted but you can encrypt attachments.

Physical & Environmental Security

- Using certified cloud providers (e.g., Microsoft, Google, AWS) will provide these controls as standard.

- Documents must be securely shredded.

- Hardware devices should be professional destroyed to ensure secure destruction.