Campbell & Kennedy Maintenance

Third Party Security Requirements Standard for Suppliers

Contents

1 Introduction 3
2 Information Security Policy 4
3 Third party organisation. 5
4 Human resources security 6
5 Third party chain management 9
6 Asset management 10
7 Physical and Environmental Security 11
8 Facilities and equipment security 13
9 Communications and operations management 14
10 Access control 19
11 Information systems acquisition, development and maintenance 19
12 Incident management 21
13 Business continuity management 22
14 Compliance 23
15 PCI-DSS compliance (where applicable) 24
16 Client protection 25
17 Documents required 26
Appendix 1 – Defined Terms 27
Document control 28

1 Introduction

Campbell & Kennedy Maintenance relies on the integrity and accuracy of its data in order to deliver its services. It is therefore paramount that the integrity, confidentiality and availability of Campbell & Kennedy Maintenance data is ensured. Any third party which processes or manages Campbell & Kennedy Maintenance Information must adhere to these principles to ensure that Campbell & Kennedy Maintenance maintains the trust of all relevant stakeholders and remains in compliance with relevant legal and regulatory requirements.

1.1 Purpose

This standard forms part of a suite of Third Party Security Standards which includes:

1. Third Party Security Compliance Standard
2. Security Standard for Production Companies
3. Security Standard for Third Parties (Content Protection)
4. Security Standard for Cloud Service Providers

This document sets out the minimum information security requirements expected of third parties who have access to Campbell & Kennedy Maintenance information during the provision of contracted services to Campbell & Kennedy Maintenance. The Standard aims to effectively protect Campbell & Kennedy Maintenance information by providing a flexible yet consistent approach to managing information security risk in third party suppliers and assist Campbell & Kennedy Maintenance suppliers to better understand and work co-operatively with Campbell & Kennedy Maintenance on proportionate security controls.

1.2 Scope

The scope of this Standard includes any third party which will process or have access to Campbell & Kennedy Maintenance information. This includes, but is not limited to:

- Third parties involved in the design, development or operation of information systems for Campbell & Kennedy Maintenance e.g. writing and installing bespoke software, third party maintenance or operation of systems, outsourcing of facilities;
- Access to Campbell & Kennedy Maintenance information from remote locations where the computer and network Users who are not employees of Campbell & Kennedy Maintenance
- This Standard therefore also applies to all staff, including contractors, temporary staff and third parties employed directly and indirectly by the Third Party organisation (e.g. subcontractors).

If there is a direct conflict between any requirements of this Standard and the terms of a written agreement between the Supplier and Campbell & Kennedy Maintenance, the terms of the written contract will prevail to the extent of the conflict.

1.3 Ownership and Document Change Control

This Standard is owned and maintained by Campbell & Kennedy Maintenance's Managed Services Department & can be amended with or without notice from time to time at Campbell & Kennedy Maintenance's discretion. Third Parties will not be expected to comply with any changes to this document until they have been provided with such changes in writing and a reasonable period (not to exceed 120 days) to comply with such changes.

The Standard will be comprehensively reviewed by Campbell & Kennedy Maintenance Information Security and updated as necessary every year.

Any queries or feedback relating to implementation or compliance should be directed to Campbell & Kennedy Maintenance's Managed Services Department (operations@ckmaintenance.co.uk)

1.4 Information Security Reviews

Third parties who fall within scope may be subject to compliance review against this Standard and will be required to comply with the requirements herein, where the controls are applicable, proportionate and appropriate.

Third parties must document any security elements and controls that have been implemented to comply with this Standard in order to assist with any information security reviews carried out by Campbell & Kennedy Maintenance or their nominated parties.

1.5 Exceptions

Campbell & Kennedy Maintenance Security Standards are in place to assist Campbell & Kennedy Maintenance's and its suppliers in complying with information security best practices and legislative and regulatory requirements. Where it is not feasible for the third party to comply with any of the specific control requirements defined in this Standard, approval will be required from Campbell & Kennedy Maintenance's Managed Services department. Each non-compliance will be evaluated and risk- assessed, and either the risk accepted by Campbell & Kennedy Maintenance Managed Services or the third party required to comply with the control and an implementation date agreed with the assistance of Campbell & Kennedy Maintenance Managed Services.

2 Information Security Policy

2.1 Information Security Policy

2.1.1 The Third Party shall at all times maintain a management-approved corporate Information Security Policy, or set of Information Security Policies, defining responsibilities and setting out the Third Party's approach to information security.

2.2 Industry standards

2.2.1 The Third Party shall at all times maintain a supporting framework of policies covering all requirements set out in this document in line with industry best-practice.

2.3 Publication and communication

2.3.1 The Third Party shall at all times ensure that its Information Security Policies are published and effectively communicated to all staff responsible for Campbell & Kennedy Maintenance Information.

3 Third party organisation

3.1 Information security function

3.1.1 The third party shall designate named individuals or teams who will have responsibility and accountability for information security policy, implementation and processes. Such nominated individuals shall act as the primary points of contact for Campbell & Kennedy Maintenance where information security is concerned. Additionally, they shall facilitate any security review meetings and manage any restoration plan in the event of a security breach.

3.2 Senior management commitment

3.2.1 The Third-Party senior management shall provide clear strategic direction and support business areas to assess, monitor and control information security risks, and ensure that information security issues raised are properly addressed.

3.3 Processes and procedures

3.3.1 Documented procedures must be in place to authorise significant changes to Campbell & Kennedy Maintenance Information processing procedures and to ensure relevant information security contacts are maintained. All processes for managing the security of Campbell & Kennedy Maintenance Information must be assessed on an annual basis and communicated to Campbell & Kennedy Maintenance's Managed Service Department.

3.3.2 The Third Party shall not process or otherwise make use of Campbell & Kennedy Maintenance information, for any purpose other than that which is directly required for the supply of the agreed Services.

3.3.3 The Third Party shall only perform such Services in accordance with the Contract.

3.3.4 The Third Party shall not purport to sell, let for hire, assign rights in or otherwise dispose of any of Campbell & Kennedy Maintenance information without the prior written approval of Campbell & Kennedy Maintenance.

3.3.5 The Third Party shall not commercially exploit Campbell & Kennedy Maintenance information or Campbell & Kennedy Maintenance Materials without the prior written approval of Campbell & Kennedy Maintenance.

3.3.6 The Third Party shall establish and at all times maintain safeguards against the accidental or deliberate or unauthorised disclosure, access, manipulation, alteration and against any destruction, corruption of, damage, loss or misuse of Campbell & Kennedy Maintenance information in the possession of the Third Party or any sub-contractors or agents of the Third Party.

3.4 Information risk

3.4.1 The Third Party shall maintain a register of the security risks related to the provision of its Services to Campbell & Kennedy Maintenance and to Campbell & Kennedy Maintenance information. Risk assessments carried out by the Third Party under its contractual obligations shall involve a senior manager with overall responsibilities for information security. The risk register shall be maintained to show the nature and extent of, and progress made in, mitigating the identified risks.

4 Human resources security

4.1 Prior to employment

Roles and responsibilities:

4.1.1 The Third Party shall ensure that information security roles and responsibilities of all Third-Party employees (and subcontractors) are clearly defined and documented.

4.1.2 The Third Party shall (and shall procure that its Subcontractors shall) have a comprehensive disciplinary policy, code of conduct & work rules directive in force to protect the interests and safety of Third Party and Subcontractor personnel and the Services, and the security of Campbell & Kennedy Maintenance personnel and information. That policy shall clearly define what breaches of security represent misconduct and what consequences shall be incurred.

Screening

4.1.3 The Third Party shall ensure that its personnel application and contractual process contain a series of declarations that the applicant must make to cover criminal convictions as per the terms of the Rehabilitation of Offenders Act 1974, pending criminal investigations or adverse financial probity judgements such as county court judgments or bankruptcy rulings.

4.1.4 The Third Party shall ensure that the application and contractual process contain a series of consents from the applicant to cover pre or post-employment ('Security Screening Waivers'), giving consent for the Third Party to obtain County Court Judgment, and/or Criminal Record reports.

4.1.5 If the declarations or the relevant Criminal Record Check, in relation to a Third Party or Subcontractor staff member who it is intended shall be involved in the provision of Services or is already involved in the provision of the Services, reveal any convictions then the Third Party shall in every case immediately bring this to Campbell & Kennedy Maintenance's attention for consultation. In such circumstances Campbell & Kennedy Maintenance shall have the right to require that the relevant staff member is removed from participating in the provision of the Services.

4.1.6 Where the Third Party's business function includes financial payment transactions, the Third Party shall ensure that a financial probity check (covering adverse County Court Judgments and bankruptcy rulings) is conducted with Experian or other reputable agency (the "Financial Probity Check") against all Third Party and Subcontractor personnel involved in the provision of the Services. If the declarations or the relevant Financial Probity Check reveal any adverse County Court Judgments or bankruptcy rulings, then the Third Party shall immediately notify Campbell & Kennedy Maintenance for consultation. In such circumstances Campbell & Kennedy Maintenance shall have the right to require that the relevant staff member is removed from participating in the provision of the Services.

4.1.7 The Third Party shall ensure that all above-mentioned background checks ("Background Checks") shall be conducted at the Third Party's cost and within a reasonable time period and in any event shall be completed prior to such Third Party or Subcontractor personnel commencing provision of the Services (excluding training). The Third Party shall bear all training and attrition costs if any Third Party or Subcontractor personnel are removed from the Services as a result of a positive disclosure on any declaration or Background Check.

Employment references

4.1.8 The Third Party shall ensure that a written policy exists and is followed for pre-employment screening and that the screening status and results for all Third Party personnel are fully collated, kept on record and made available to Campbell & Kennedy Maintenance on Campbell & Kennedy Maintenance's written request for audit andcompliance

4.1.9 The Third Party shall obtain two references prior to its personnel completing training and commencing work. Such references may be verbal, but must be verified, fully documented and auditable. Where reasonably possible, the Third Party shall obtain at least one such reference from a previous employer or academic professional.

Contractual agreements

4.1.10 The Third Party shall ensure that all personnel enter into a written contract of employment under which they agree to adhere to all Third Party policies, rules and procedures including all information protection policies and agree to assign all intellectual property created in the course of providing the Services to the Third Party so that the intellectual property provisions of the Contract can take effect.

4.1.11 The Third Party shall ensure that all personnel working in the provision of the Services sign an appropriate employee non-disclosure agreement relating to Campbell & Kennedy Maintenance information in the possession of the Third Party before they are given access to any such Campbell & Kennedy Maintenance Information.

4.2 During employment

New Employee Induction

4.2.1 The Third Party shall ensure that a Security module forms part of the compulsory induction and training programme for all Third-Party personnel involved in the provision of the Services. Such security module shall be sufficient to include information protection and security, the password and user account policy, issues of confidentiality and company security standards.

4.2.2 The Security Module shall as a minimum:

- Define the meaning and importance of information security;
- Underline the importance of complying with relevant information security policies and procedures and applying information security practices when processing Campbell & Kennedy Maintenance Information.
- Outline employee and Third-Party responsibilities for the protection of Campbell & Kennedy Maintenance Information including reporting suspected and actual information security incidents with regards to Campbell & Kennedy Maintenance Information.
- Make clear the consequences and disciplinary procedures for not complying with this policy.

Compliance with policy

4.2.3 The Third Party shall ensure that all employees and Third Parties have read, understood and remain in compliance with applicable third-party security policies and procedures.

4.2.4 The Third Party shall invoke a formal disciplinary process for its employees who have committed a security breach and shall ensure that its Subcontractors will do the same.

Training and awareness

4.2.5 The Third Party shall hold structured briefings with respect to security awareness and knowledge of fraud and security issues (focusing on the risks resulting from poor information security, and legal and regulatory requirements to protect information) with Third Party personnel and its Subcontractors throughout the provision of the Services and shall review such briefing requirements on a regular basis.

4.2.6 The Third Party shall ensure that all Third-Party personnel (including Subcontractor personnel) have the appropriate skills and training to support the Services, and that all IT or Information Security personnel (including Subcontractor personnel) have been given the authority and training to appropriately discharge their responsibilities.

Disciplinary procedure

4.2.7 Formal disciplinary procedures must be in place for employees and Subcontractors who breach any applicable security policy related to the protection of Campbell & Kennedy Maintenance information.

4.2.8 The Third Party shall consult Campbell & Kennedy Maintenance Information Security where any of its personnel (or any Subcontractor personnel) are subject to a change of circumstance and are then assessed to be a risk to the Services or Campbell & Kennedy Maintenance Information.

4.3 Termination of employment

4.3.1 The Third Party shall carry out a 'checklist' of actions, including exit interview where appropriate, prior to the conclusion of the departing personnel's employment and shall ensure that any Subcontractor shall do the same. This checklist of actions shall include cancellation of access control privileges and user IDs/passwords required for access to the Third Party (and/or Subcontractor) and Campbell & Kennedy Maintenance Systems and recovery of any asset(s) that may contain information relating to Campbell & Kennedy Maintenance and/or Campbell & Kennedy Maintenance Associated Company and all property of same *(including but not limited to books, correspondence, files, statistics, papers, reports, minutes, plans, records, surveys, diagrams, computer print-outs, computer disks, CDs, audio tapes, manuals, customer documentation or any other medium for storing information in whatever form*), and any swipe cards or ID passes giving the departing personnel access to Third Party (and/or Subcontractor) or Campbell & Kennedy Maintenance premises or storage or both; and deletion of data relating in any way to Campbell & Kennedy Maintenance and/or Campbell & Kennedy Maintenance Associated Company stored on any asset or system which is not a Campbell & Kennedy Maintenance or Campbell & Kennedy Maintenance Associated Company system.

5 Third party chain management

Authorised access

5.1.1 The Third Party shall provide full details of any Subcontractor(s) that it intends to use in the provision of the Services; such details to include as a minimum company name, address, location, and type of Services to be provided and the volume, frequency and nature of Campbell & Kennedy Maintenance information to be used.

5.1.2 The Third Party shall not make Campbell & Kennedy Maintenance information available to any Subcontractor without the prior written approval of Campbell & Kennedy Maintenance.

Risk-assessed access

5.1.3 The third party must carry out an information security risk assessment prior to any Third-Party access and the results of this must also be submitted to Campbell & Kennedy Maintenance's Managed Services Department.

5.1.4 The Third Party shall ensure that it is not reliant on any key single individual to support Services anywhere in its supply chain.

Controlled access

5.1.5 The Third Party shall ensure that all Subcontractor agreements contain security controls, service definitions, service requirements and delivery levels commensurate with the requirements set out in this document, and that such are implemented, operated, and maintained by all Subcontractors at all times.

Security accountability

5.1.6 The security relationship with each Third Party must be allocated to a named member of Third-Party staff with senior management accountability.

Compliance

5.1.7 The Third Party shall conduct annual security reviews of the Subcontractors where those Subcontractors have access to Campbell & Kennedy Maintenance information, and maintain detailed, written evidence of these audits to include any security risks, recommendations and remedial actions.

5.1.8 Third Party security reviews shall be conducted in accordance with the requirements set out in this document.

Contractual agreements

5.1.9 Third Party Subcontractors must operate in accordance with non-disclosure clauses stipulated in agreements between the Third Party and the Subcontractor.

Contract termination

5.1.10 Exit procedures and requirements must be included in any agreement between the Third Party and the Subcontractor and all Third-Party access to Campbell & Kennedy Maintenance information must be revoked when no longer required.

6 Asset management

6.1 Information classification

6.1.1 The Third Party shall ensure that Campbell & Kennedy Maintenance Information is classified in terms of its value, legal requirements, sensitivity and criticality.

6.1.2 The Third Party shall ensure that an appropriate set of procedures for information labelling and handling is developed and implemented in accordance with the classification scheme adopted by the Third Party, and that such procedures are reviewed as a result of any significant business changes.

6.2 Information handling

6.2.1 Third Party management must be aware and take ownership of information assets and produce a policy to enforce correct use of the assets. An information asset includes, but is not limited to, physical and logical information assets.

Asset inventory

6.2.2 All information assets used to process Campbell & Kennedy Maintenance Information must be recorded in a maintained inventory. All Third-Party Subcontractors must also maintain a similar inventory.

6.2.3 The Third Party shall ensure that any media used to record, store or process Campbell & Kennedy Maintenance Information as part of the Services, including (but not limited to) hard copy output, laptops, USB sticks, pen drives, CDs, or other magnetic media are securely handled, transported and encrypted and that their use is authorised.

Asset ownership

6.2.4 All information assets used to process Campbell & Kennedy Maintenance Information must be owned by a designated officer of the Third Party organisation.

Acceptable Use Policy (AUP)

6.2.5 An AUP must be defined and communicated to all users processing Campbell & Kennedy Maintenance Information. The AUP must:

1. Define appropriate use of communications channels and devices used to process Campbell & Kennedy Maintenance Information;

2. Define appropriate use of the Internet, including prohibiting the transfer of Campbell & Kennedy Maintenance Information to personal email accounts or unauthorised cloud-based storage;

3. include responsibilities relating to downloading, installing and use of unauthorised or illegal software or material to process Campbell & Kennedy Maintenance Information.
4. make clear statements about consequences of non-compliance or breach of the AUP; and
5. be communicated to Campbell & Kennedy's Managed Services Department.

7 Physical and Environmental

7.1 Policy

7.1.2 The Third Party shall (and shall ensure that its Subcontractors shall) implement a policy identifying the requirements for physical access and control of such access of its Sites (or those of the Subcontractor from where Services are provided).

7.1.3 Without prejudice to any of Campbell & Kennedy Maintenance's remedies, sanctions against Third Party and Subcontractor staff for breaches of security requirements shall be governed by the Third Party's or the Subcontractor's disciplinary policy as appropriate.

7.2 Physical site

7.2.1 If a new site is to be selected, Campbell & Kennedy Maintenance's Managed Services Department should be included as part of the initial assessment and approval team.

7.2.2 The Third Party will not perform the Services from other locations without obtaining the prior written consent of Campbell & Kennedy Maintenance, and any relocation will be approved by and implemented at no additional cost to Campbell & Kennedy Maintenance (unless any relocation is due to a specific request from Campbell & Kennedy Maintenance) and without causing any material disruption to the business of Campbell & Kennedy Maintenance or the Services.

Site changes

7.2.3 Significant changes to sites processing Campbell & Kennedy Maintenance Information must be approved by Campbell & Kennedy Maintenance's Managed Services Department.

Shared site

7.2.4 Where Campbell & Kennedy Maintenance agrees (either under the Contract or by prior written consent) to a shared site, the Third Party shall as a minimum:

- Segregate the area in which the Services are performed for Campbell & Kennedy maintenance; Implement a clearly defined area for performing the Services;
- ensure that the Services and facilities required to provide the Services to Campbell & Kennedy Maintenance are kept completely physically separate from the Third Party's other clients with dedicated exit/entrance points and clear divides as defined by partition walling or desk plans.

Secure perimeter

7.2.5 The Third Party shall (and shall ensure that its Subcontractors shall) review the strength and effectiveness of the management of physical security controls at its

Sites (or those of its Subcontractors from where the Services are provided) at least every six months.

7.2.6 Where an automated access control system is deployed at its Sites (or those ofits Subcontractors from where the Services are provided), the Third Party shall (and shall ensure that its Subcontractors shall) ensure that the system logs all access control events and that this log is audited on an on-going basis.

7.2.7 In the event that such automated access control system is not able to check and verify all staff and contractors ID passes and/or prevent tailgating, the Third Party shall (and shall ensure that its Subcontractors shall) deploy a physical security function or other mitigating control to enforce compliance in this area.

7.2.8 The Third Party shall ensure that all Third-Party personnel (and any Subcontractor personnel) are issued with unique ID passes from which they are individually identifiable, and which shall then be worn and visible at all times. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.9 The Third Party shall be responsible for retrieving the ID passes of any Third-Party personnel (and any Subcontractor personnel) that have had their employment terminated, transferred or otherwise no longer require access to the Site(s). The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.10 The Third Party shall ensure that a robust policy is in force to manage loss of ID passes and ID passes left at home by Third Party personnel (and any Subcontractor personnel). The Third Party shall ensure that its Subcontractors will enforce a similar policy at any Subcontractor sites from where the Services are provided.

7.2.11 The Third Party shall operate a sign-in procedure for any visitors to the Sites, which, as a minimum, requires visitors to log their name, company, the time and date and the name of the person whom they are visiting at the relevant Sites. The Third Party shall ensure that its Subcontractors will operate a similar procedure at any Subcontractor sites from where the Services are provided.

7.2.12 The Third Party shall deny entry to visitors to the Sites who are not legitimately connected with the Services being performed unless they are duly authorised to do so by the appropriate Third-Party management. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.13 The Third Party shall inform all visitors of the existence of Site security policies. The Third Party shall ensure that its Subcontractors will inform all visitors of the existence of site security policies at any Subcontractor sites from where the Services are provided.

7.2.14 The Third Party shall ensure that there is a manned guarding or other appropriate physical security presence on Sites which are processing or storing Sensitive Campbell & Kennedy Maintenance Information. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.15 The Third Party shall ensure that there is a physical security response capability during out of hours periods for those Sites storing or processing Sensitive Campbell & Kennedy Maintenance Information. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.16 The Third Party shall ensure security response personnel receive appropriate training in all security related policies. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.17 The Third Party shall ensure security response personnel are instructed to take action as appropriate or escalate the incident to a manager. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.18 The Third Party shall have in place an internal and external CCTV system with sufficient coverage to monitor reception areas, exit/entry points, and vulnerable or sensitive/confidential working areas. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

7.2.19 The Third Party shall implement, operate, support, and maintain alarm systems (including appropriate environmental alarms), and physical access mechanisms. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites from where the Services are provided.

8 Facilities and equipment security

8.1.1 Equipment used to process Campbell & Kennedy Maintenance Information must be secured against unauthorized logical or physical access.

8.1.2 The Third Party shall (and shall ensure that its Subcontractors shall) provide and maintain suitable accommodation, facilities, equipment, space, furnishing, utilities and fixtures necessary to provide secure physical premises that provide a safe working environment from which to provide the Services to Campbell & Kennedy Maintenance and that adequately protects against any loss or damage to the premises or to the equipment.

8.1.3 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that power and telecommunications cabling carrying Campbell & Kennedy Maintenance Information or supporting information services in relation to the Services are routed appropriately and protected where vulnerable to attack, interception or damage.

8.1.4 The Third Party shall (and shall ensure that its Subcontractors shall) implement uninterruptible power supplies ("UPS") for critical infrastructure in relation to the Services and shall test the UPS regularly.

8.1.5 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that all power supplies and fire safety mechanisms in facilities from which Services are provided undergo regular maintenance checks and that facilities comply with Health and Safety regulations.

8.1.6 Where Campbell & Kennedy Maintenance Information is stored or processed by the Third Party (or any Subcontractor), the Third Party shall (and shall ensure that the Subcontractor shall)

provide sufficient secure storage space for its personnel to store those personal effects that are capable of capturing and storing Campbell & Kennedy Maintenance information and shall ensure that personnel utilise such storage space.

8.1.7 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that prominent security signage detailing security policies and requirements are provided and displayed in all facilities from which the Services are provided.

8.1.8 The Third Party shall ensure a clear desk policy is operated and maintained within the Sites where Campbell & Kennedy Maintenance Information is stored or processed. The Third Party shall ensure that its Subcontractors will do the same at any Subcontractor sites where Campbell & Kennedy Maintenance Information is stored or processed.

9 Communications and operations

9.1 Operating procedure documentation

9.1.1 Operating procedures for information security management and controls related to Campbell & Kennedy Maintenance Information must be documented, maintained and made available to the relevant user involved in processing Campbell & Kennedy Maintenance Information.

9.2 Operational separation of duties

9.2.1 Duties and areas of responsibility must be segregated to reduce opportunities for unintentional or unauthorised modification or misuse of Campbell & Kennedy Maintenance Information.

9.2.2 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that development, testing, production and operational facilities are separated to reduce the risks of unauthorised access or changes to the operational system.

9.3 Malware protection

Malware incident response

9.3.1 The Third Party shall promptly notify Campbell & Kennedy Maintenance in writing as soon as it becomes aware of any viruses in any Third Party Systems or Campbell & Kennedy Maintenance Systems, directly (or indirectly) affecting Campbell & Kennedy Maintenance Information, which have not been auto-corrected or detected and quarantined, and shall provide a written report to Campbell & Kennedy Maintenance describing the incident, the measures that were taken to resolve the incident and what measures were taken to prevent any reoccurrence.

Malware protection tool

9.3.2 The Third Party shall provide anti-virus protection software on all Third-Party Systems vulnerable to virus infection and shall ensure that its Subcontractors shall do the same on any Subcontractor systems used in the provision of the Services in accordance with the requirements of this standard. The Third Party shall (and shall ensure that its Subcontractors shall) use all reasonable endeavours to detect hidden code or information that is designed to, or will have the effect of:

- destroying, altering, corrupting or facilitating the theft of any Campbell & Kennedy Maintenance Information; or
- disabling or locking any software or Third-Party Systems or Campbell & Kennedy Maintenance Systems; or

- using undocumented or unauthorised access methods for gaining access to Campbell & Kennedy Maintenance Information, or Third Party or Campbell & Kennedy Maintenance Systems.

9.3.3 The Third Party shall ensure that anti-virus software and anti-virus definition files are updated for all Third-Party Systems in line with best business practice and in accordance with advice from applicable anti-virus software. The Third Party shall also ensure that its Subcontractors shall do the same on any Subcontractor systems used in the provision of the Service.

9.3.4 The Third Party shall ensure that the malware protection tool deployed:

- is a current and supported version;
- is updated with definition or signature files on a daily basis as a minimum;
- provides real time on-access and on-demand scanning;
- scan all content entering and leaving the IT infrastructure processing Campbell & Kennedy Maintenance Information;
- is able to disinfect, quarantine or delete malware;
- can provide logging, alerts and reporting functionality; and
- cannot be disabled, reconfigured or prevented from working by unauthorised users.

Malware protection on devices

9.3.5 The Third Party shall ensure that, where technically feasible, any device processing CA Information must run the malware protection tool. This includes, but is not limited to, workstation, portable devices and servers. Where devices are technically unable to run the malware protection tool, then alternative mitigations shall be put in place to provide malware protection within the information processing chain.

9.4 Data back-up

9.4.1 The Third Party shall ensure that regular backups of all Third-Party Systems hosting Campbell & Kennedy Maintenance information are performed, and their restoration tested, dependent on the frequency of information change.

9.4.2 The Third Party shall ensure that where Third Party Systems backups are stored off-site they are encrypted and securely transported, and a written register maintained of all backup tapes stored off-site.

9.4.3 The Third Party shall have processes in place ensure the recovery from the loss or damage of Campbell & Kennedy Maintenance Information or facilities used to process Campbell & Kennedy Maintenance Information.

9.4.4 The third party shall operate a back-up policy which mandates:

- the backing-up of Campbell & Kennedy Maintenance Information at scheduled risk-
- based intervals;
- validation of the back-ups;
- back-up retention periods;
- back-up type;
- media cycles and labelling; and

9.4.5 The Third Party's back-up policy must be approved by Campbell & Kennedy's Managed Services Department.

9.5 Network security management

9.5.1 The Third Party shall (and shall ensure that its Subcontractors shall) maintain the appropriate confidentiality, integrity, and availability of Campbell & Kennedy Maintenance Information, by:

- utilising secure network architecture and operations;
- ensuring that networks carrying Campbell & Kennedy Maintenance Information are designed, built, monitored, and managed according to industry standards, best practices and frameworks e.g. ISO27001, TOGAF, OWASP ITIL, etc. such that they enforce the required information security policy boundaries. These boundaries must prevent unauthorised access to Systems and Campbell & Kennedy Maintenance Systems or Campbell & Kennedy Maintenance Information by default and allow only explicitly authorised and authenticated access.

9.5.2 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that anti-virus and firewall protection systems are implemented in relation to both internal and external traffic and ensure that:

- firewall platforms are hardened;
- penetration tests of firewall protected network connections are conducted by trained personnel on a regular basis;
- firewalls have real-time logging and alerting capabilities;
- intrusion detection systems are implemented where Internet connections exist;
- access lists are implemented on network routers to restrict access to sensitive internal networks or servers.

9.5.3 Remote support access shall be controlled via a secure gateway that implements the following controls:

- strong mutual authentication (e.g. two-factor authentication);
- access via a secure gateway (e.g. a firewall);
- remote support accounts only enabled for the duration of troubleshooting activity;
- all troubleshooting activity is logged and reviewed.

9.5.4 The Third Party shall seek prior written Campbell & Kennedy Maintenance approval to use any third-party provider of remote support of Third-Party systems. Any such approved Subcontractor shall be subject to a contract between the Third Party and such Subcontractor detailing security requirements in relation to such support, and that
access granted to the Subcontractor in order to provide such support is given with minimum privileges and revoked on completion.

9.5.5 The Third Party shall develop and implement an appropriate internet, email and acceptable use policy and ensure that appropriate controls are in place and documented to prevent unauthorised download of software or web content by Third Party (or Subcontractor) personnel.

9.5.6 The Third Party shall ensure that utility programs capable of overriding system and application controls shall be restricted and tightly controlled.

9.5.7 The Third Party shall ensure that automatic equipment identification shall be used where appropriate as a means to authenticate connections from specific locations and equipment.

9.5.8 The Third Party shall have in place an intrusion detection strategy and upon request by Campbell & Kennedy Maintenance, provide written evidence as to what methods are employed, whether these are recognised intrusion detection systems or whether there is a reliance on other controls in place (firewalls, network router/switch protection) and whether the function is outsourced.

9.5.9 The Third Party shall ensure that regular penetration testing is carried out and shall agree in writing beforehand the scope of penetration testing for the Services with Campbell & Kennedy maintenance. Further, the Third Party shall notify Campbell & Kennedy Maintenance in writing of the results of such testing and take action on the recommendations in timescales commensurate with the associated risks.

9.6 Platform and application security

9.6.1 The Third Party shall (and shall ensure that its Subcontractors shall) ensure:

- that standard platform builds are documented;
- all unnecessary services are removed from platforms or disabled, and remaining settings and software are security hardened;
- policies and procedures are developed and implemented to protect Campbell & Kennedy Maintenance Information associated with the interconnection of Third Party and Campbell & Kennedy Maintenance Systems; and
- all software installed on platforms is fully licensed and its use is authorised.

9.6.2 Where financial transactional functionality is (or becomes) a part of the Services, the Third Party shall provide information masking functionality in relation to software in respect of any financial information (including but not limited to debit/credit card and direct debit banking information) which Third Party (or its Subcontractors) handles for, or on behalf of Campbell & Kennedy Maintenance.

9.7 System management

9.7.1 The Third Party shall (and shall ensure that its Subcontractors shall) maintain Systems security measures to guard against the accidental, deliberate or unauthorised disclosure, access, manipulation, alteration, destruction, corruption of information through processing errors, damage or loss or misuse of Campbell & Kennedy Maintenance Information. As a minimum, these measures shall include software which:

- requires all users of the Systems to enter a username or identification number and password prior to gaining access to the Systems;
- controls and tracks the addition and deletion of users of Systems; and
- controls, logs and tracks user access to areas and features of the Systems.

9.7.2 The Third Party shall provide Campbell & Kennedy Maintenance with a written record of such user access from time to time where Campbell& Kennedy Maintenance reasonably requests such information.

9.7.3 The Third Party shall update, monitor and review all of the Third-Party Systems regularly.

9.7.4 The Third Party shall ensure that Third Party System clocks are synchronised with an agreed accurate time source.

9.7.5 The Third Party shall ensure that sufficient physical and logical segregation is applied to any equipment operated by the Third Party for Services provided to Campbell & Kennedy unless explicit written authorisation is given by Campbell & Kennedy Maintenance for exceptions.

9.7.6 The Third Party shall ensure that the Services are fully resilient unless Campbell & Kennedy Maintenance has confirmed in writing that this is not required.

9.7.7 The Third Party shall ensure that any faults are logged, investigated, prioritised and rectified in timescales commensurate with the associated risks.

9.8 Mobile computing

9.8.1 The Third Party shall ensure that it adopts a policy to protect against the risk of using mobile computing, teleworking activities and communication facilities where these are used to deliver Services to Campbell & Kennedy Maintenance.

9.9 Data encryption

9.9.1 The Third Party shall transfer/exchange Campbell & Kennedy Maintenance Information via secure channels which are encrypted and further shall inform Campbell & Kennedy Maintenance in writing of the encryption solution used to transfer/exchange Campbell & Kennedy Maintenance Information in advance of any transfer or exchange. This solution must be in compliance with Campbell & Kennedy Maintenance's Data Encryption Policy and is also applicable to Campbell & Kennedy Maintenance Restricted Data stored at off-site facilities.

9.9.2 All such transfer/exchange of Campbell & Kennedy Maintenance Information shall be compliant with all relevant agreements, laws, regulations and current industry best practice.

9.10 Monitoring and audit logs

9.10.1 Procedures must be in place to actively monitor for, review and act on any unauthorised processing of Campbell & Kennedy Maintenance Information.

9.10.2 Auditing of activities and information security events related to the processing of Campbell & Kennedy Maintenance Information must be kept in a secure log files which are protected against unauthorised alteration or deletions and are backed-up in line with the back-up policy.

9.10.3 The logged information must include fields that are attributable to a single individual to ensure accountability and must be kept for an agreed time to assist with any possible investigations. Logs must be made available to Campbell & Kennedy Maintenance Information Security on request either as real-time or batch.

10 Access control

10.1 Access

10.1.1 The Third Party shall have an established, documented, and regularly reviewed formal procedure for the provision and limitation of access to the Third-Party Systems, any Campbell & Kennedy Maintenance Systems, and Campbell & Kennedy Maintenance Information so that access is limited to those personnel that need access to such information or systems to perform their duties.

10.2 Passwords

10.2.1 The Third Party shall have a system-enforced password and user account policy that meets or exceeds Campbell & Kennedy Maintenance password policy, i.e. minimum password length, strength; minimum and maximum age and password reuse prevention. This shall include procedures to be followed when personnel leave their workstation and a process to control and manages user accounts upon completion of employment or an individual's short term contract or a change in role.

10.2.2 An automated system lock is to be invoked by where a workstation used to access, or process Campbell & Kennedy Maintenance Information is left unattended for a period in excess of 10 minutes.

10.2.3 The Third Party shall ensure that restrictions on connection times shall be used to provide additional security for high risk applications processing Sensitive Campbell & Kennedy Maintenance Information.

10.2.4 The Third Party shall ensure that all platform and application user accounts are unique, justified, authorised and regularly reviewed and:

- all platform accounts are granted minimum privileges;
- significant platform activity is logged in writing and regularly reviewed;
- access to platform audit trails is restricted and logged;
- default accounts are deleted or disabled;
- privileged platform accounts, e.g. root, are only used under change control procedures and not for day-to-day system operation;
- where privileged account access is used, this access is logged in writing and regularly reviewed;
- access to databases is restricted;
- where SQL databases are implemented, recent vulnerabilities are patched or mitigated;
- access to information systems audit tools shall be appropriately protected to prevent any possible misuse or compromise.

11 Information systems acquisition, development and maintenance

11.1 Security requirements for Information Systems

11.1.1 New information systems or enhancements to existing systems must have valid business requirements which must specify security controls to maintain or protect

Campbell & Kennedy Maintenance Information. The business requirements must be agreed by Campbell & Kennedy Maintenance's Managed Service's department and must be subject to the third parties defined risk managementprocess.

11.1.2 The Third Party shall ensure that any new systems introduced into Campbell & Kennedy Maintenance's Information environment are compliant with PCI DSS (where applicable), the requirements of the Data Protection Act 2018 (and any amendment thereof or replacement thereto) and any other relevant legal and regulatoryrequirements.

11.1.3 Capacity requirements must take into account the business criticality of the system. Procedures must require information systems to be designed to cope with current and predicted information processing requirements. The Third Party shall ensure that capacity requirements are monitored, and Third-Party Systems and networks are regularly reviewed so that they are scaled accordingly.

11.1.4 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that where cryptographic controls are implemented, procedures for the use of cryptography and key management are in line with Campbell & Kennedy Maintenance Data Encryption Policy, are securely managed using documented policy procedures, and key changes made under dual control.

11.2 Security in development, change and support processes

11.2.1 A policy document to outline a secure process for software development of software and systems processing Campbell & Kennedy Maintenance Information, whether in-house or outsourced, needs to be defined andmaintained.

11.2.2 Technical security standards (including secure build configuration) for applications and systems used in processing Campbell & Kennedy Maintenance Information must be defined, documented and maintained. New systems and applications must comply with these standards.

11.2.3 The Third Party shall ensure that change control procedures are agreed and documented between the Third Party and Campbell & Kennedy Maintenance; and that such documented procedures require that detail as to why the change was required and how and when the changes were executed are recorded and also include an emergency change process.

11.2.4 The Third Party shall notify Campbell & Kennedy Maintenance of any upgrades or configuration changes which will impact on the security of Campbell & Kennedy Maintenance Information, including (but not limited to) payment card information which as such may affect the PCI DSS compliance status of the Third Party andServices.

11.2.5 The Third Party shall ensure that back out procedures are documented priorto implementing anychange.

11.2.6 The Third Party shall ensure that all changes for information systems, upgrades, and new software in relation to the Services have considered security control requirements, based upon the identified risks, and that these changes are tested prior to implementation.

11.2.7 The Third Party shall ensure that access to program source code is restricted and strictly controlled

11.3 Technical vulnerability management

11.3.1 The Third Party shall have in place an intrusion detection strategy and upon request by Campbell & Kennedy Maintenance, provide written evidence as to what methods are employed, whether these are recognised intrusion detection systems or whether there is a reliance on other controls in place (firewalls, network router/switch protection) and whether the function is outsourced.

11.3.2 The Third Party shall ensure that regular penetration testing is carried out and shall agree in writing beforehand the scope of penetration testing for the Services with Campbell & Kennedy Maintenance. Further, the Third Party shall notify Campbell & Kennedy Maintenance in writing of the results of such testing and take action on the recommendations in timescales commensurate with the associated risks.

11.3.3 The Third Party shall (and shall ensure that its Subcontractors shall) ensure that appropriate patch management procedures are in place to remain current with platform security fixes and to ensure adequate testing is carried out.

12 Incident management

12.1 Policy and Procedure

12.1.1 The Third Party shall (and shall ensure that its Subcontractors shall) at all times maintain a security incident response procedure.

12.1.2 The Third Party shall ensure that mechanisms are in place to enable the types, volumes and costs of information security incidents to be quantified and monitored. Where required by Campbell & Kennedy Maintenance, the Third Party will provide such information regarding information security incidents to Campbell & Kennedy Maintenance.

12.1.3 The Third Party shall require all Third-Party personnel (and any Subcontractor personnel) to report any observed or suspected security weaknesses in Systems or Services to the Third Party. The Third Party shall inform Campbell & Kennedy Maintenance immediately about any such weaknesses of which it becomes aware.

12.2 Reporting

12.2.1 In the provision of Services to Campbell & Kennedy Maintenance and as part of the security incident response procedure, if the Third Party becomes or is made aware of any contravention of the information security requirements under the Contract, or of unauthorised access to Campbell & Kennedy Maintenance Systems, Campbell & Kennedy Maintenance information or any Campbell & Kennedy Maintenance Systems including the Campbell & Kennedy Maintenance network, the Third Party shall (and shall ensure that its Subcontractors shall):

- immediately report the incident to Campbell & Kennedy Maintenance Information Security;
- promptly provide Campbell & Kennedy Maintenance with a detailed written report setting out the details of and reasons for the contravention of the information security requirements and describing in detail any Campbell & Kennedy Maintenance Information, Systems and/or Campbell & Kennedy Maintenance Systems which have been accessed without authorisation;

- provide Campbell & Kennedy Maintenance, at no additional cost, with any assistance to restore Campbell & Kennedy Maintenance Information, the Systems and Campbell & Kennedy Maintenance Systems and any other assistance that may be required by Campbell & Kennedy Maintenance.
  preserve evidence to include collection, retention and presentation of such evidence to Campbell & Kennedy Maintenance Information Security
- Promptly return to Campbell & Kennedy Maintenance any copied or removed Campbell & Kennedy Maintenance Information; comply with all reasonable directions of Campbell & Kennedy Maintenance and take immediate remedial action to secure Campbell & Kennedy Maintenance Information Systems and /or Campbell & Kennedy Maintenance Systems and to prevent reoccurrences of the same or similar contravention and
  provide Campbell & Kennedy Maintenance with details of such remedial action.

12.2.2 If either a criminal situation or a breach of Third Party policies and the requirements in the Contract occurs involving Third Party or Subcontractor personnel who are providing Services to Campbell & Kennedy Maintenance and such criminal situation or breach becomes known to the Third Party (or its Subcontractor), Campbell & Kennedy Maintenance must be notified as soon as practicable of the facts surrounding the same.

13 Business continuity management

13.1.1 The Third Party shall (and shall ensure that its Subcontractors shall) comply with Campbell & Kennedy Maintenance Business Continuity Policies as attached to the Contract or notified to the Third Party from time to time.

13.1.2 The Third Party shall (and shall ensure that its Subcontractors shall) align the Services delivered to Campbell & Kennedy Maintenance with a tier or tiers (as appropriate) in line with standard industry practice.

13.1.3 The Third Party shall (and shall ensure that its Subcontractors shall) should align where possible with Business Continuity Standard ISO22301.

13.1.4 The Third Party shall ensure that a Business Continuity Plan is in place in relation to the provision of Services to Campbell & Kennedy Maintenance. The plan shall set out how business operations shall be restored following an interruption to or failure of business processes within a time period agreed to be acceptable by Campbell & Kennedy Maintenance.

13.1.5 The Business Continuity Plan shall include arrangements to inform and engage appropriate Campbell & Kennedy Maintenance personnel in its execution.

13.1.6 The Third Party shall test the Business Continuity Plan at least annually and shall report back to Campbell & Kennedy Maintenance on such testing where required by Campbell & Kennedy Maintenance.

13.1.7 The Third Party shall at least annually review and update, as necessary, the Business Continuity Plan and shall submit any proposed updates to the Business Continuity Plan for Campbell & Kennedy's written, prior approval.

14 Compliance

14.1 Data privacy

14.1.1 The Third Party shall at all times ensure that it maintains and abides by an appropriate Data Protection Policy to safeguard Campbell & Kennedy Maintenance Information in accordance with the terms of the Contract and the Data Protection Act 1998 (and any amendment thereto or replacement thereof) and any other applicable statute, regulation or industry code.

14.1.2 Where any Campbell & Kennedy Maintenance Information is intended to be transferred, stored or processed outside of the UK, the Third Party shall provide (prior notice), for Campbell & Kennedy Maintenance written approval, full details of the locations, security arrangements and what information is to be transferred, stored or processed outside of the UK.

14.1.3 Where any elements of service delivery are proposed to be offshored, the proposal must be subject to a full information security risk assessment and must be approved by Campbell & Kennedy Maintenance Managed Services, and if necessary, reviewed by Campbell Kennedy legal counsel, before it can proceed.

14.1.4 The Third Party shall ensure that appropriate retention and secure deletion/destruction policies and procedures are in place for all Campbell & Kennedy Maintenance Information held. Campbell & Kennedy Maintenance may require a copy of the policies and procedures.

14.1.5 The Third Party shall maintain an information retention & destruction policy to ensure that Campbell & Kennedy Maintenance Information is retained for no longer than necessary and
is protected from unauthorised or unlawful processing. Where the Third Party is acting as a data processor (as defined under the Data Protection Act 1998 (and any amendment thereto or replacement thereof)) for the Services, they must act only in accordance with Campbell & Kennedy's instructions on retention and destruction.

14.1.6 The Third Party shall ensure that the storage and subsequent destruction of Campbell & Kennedy Maintenance Information is secure and in compliance with Campbell & Kennedy's instructions. All items of equipment used in the provision of the Services containing storage media shall be checked by the Third Party to ensure that any Campbell & Kennedy Maintenance Information and licensed software has been removed or securely overwritten prior to secure deletion.

14.1.7 If Campbell & Kennedy Maintenance Information is to be shared with a Sub-contractor, the Third Party shall notify Campbell & Kennedy Maintenance in advance and provide Campbell & Kennedy Maintenance with a copy of the legal agreement in place.

14.2 Legal, regulatory and contractual compliance

14.2.1 Legal, regulatory or contractual requirements must be complied with and taken into account in the processing of Campbell & Kennedy Maintenance Information. In particular, this includes, but is not limited to compliance with the Data Protection, Freedom of Information and privacy requirements.

14.3 Compliance with Campbell & Kennedy Maintenance policies and standards

14.3.1 Campbell & Kennedy Maintenance Information processing systems including databases processing Campbell & Kennedy Maintenance Information must be checked on an annual basis to ensure they comply with relevant security procedures including thispolicy.

14.3.2 An annual report on the compliance of Campbell & Kennedy Maintenance Information processing systems against the relevant information security standard and this policy must be provided to Campbell & Kennedy's Managed Services Department.

14.4 Audit

14.4.1 The Third Party shall grant to Campbell & Kennedy Maintenance such access to the Sites used as is necessary to allow Campbell & Kennedy Maintenance to perform its responsibilities or exercise its rights under the Contract and shall participate in information security reviews as and when reasonably requested by Campbell & Kennedy Maintenance.

14.4.2 If an investigation or audit is conducted by Campbell & Kennedy Maintenance or on behalf of Campbell & Kennedy Maintenance, the Third Party will ensure that all personnel shall cooperate with such investigators or auditors and, if requested, will make relevant personnel available for interview.

14.4.3 On or after termination of the Services, the Third Party shall grant Campbell & Kennedy Maintenance the right to perform reasonable audits and inspections of the Third Party and its Subcontractors for reasons of security, fraud and regulatory compliance in relation to the Services; or for reason of verifying the Third Party's compliance with the Contract.

14.4.4 If the Third Party has attained external validation(s) or certification(s) to any security industry standards, for example, this may include certification or standards such as ISO 27001, PCI DSS, SSAE 16 or FSA, or any other audit standards which may contain security control assessments, the Third Party shall provide evidence of the relevant certification and/or Statement of Applicability upon reasonable request.

15 PCI-DSS compliance (where applicable)

15.1.1 Where financial transactional functionality is (or becomes) a part of the Services, the Third Party shall comply with the latest version of PCI DSS requirements and provide evidence of PCI compliance through external certification or self-assessment declaration.

15.1.2 The Third Party shall maintain a written strategy for PCI DSS compliance in accordance with the Third-Party corporate Information Security Policy, which addresses each of the PCI DSS requirements, and shall assign responsibility for PCI DSS to a compliance function.

15.1.4 The Third Party shall ensure that a current network configuration diagram is produced and maintained to show clear information flows and to ensure that all connections are identified, including traffic traversing wireless networks.

15.1.5 Third Party shall not disclose Campbell & Kennedy's payment card transactions to any third party or entity, with the exception of where this is authorised by Campbell & Kennedy Maintenance under the provisions of the Contract or by prior written consent.

15.1.6 Upon request by Campbell & Kennedy Maintenance, the Third Party shall provide to Campbell & Kennedy Maintenance a written account of the scope of the environment that is included in the PCI-DSS assessment (e.g. Internet access points, internal corporate network).

15.1.7 Upon request, the Third Party shall provide to Campbell & Kennedy Maintenance written details around any gap analysis that has been produced either internally or by a PCI DSS Qualified Security Advisor (QSA). This shall include the provision of details of the most recent Self- Assessment Questionnaire or Report on Compliance.

15.1.8 Upon request by Campbell & Kennedy Maintenance, the Third Party shall provide to Campbell & Kennedy Maintenance written details of results of the last four quarterly network vulnerability scans.

15.1.9 Upon request by Campbell & Kennedy Maintenance, the Third Party shall provide to Campbell & Kennedy Maintenance, written details around any compensating controls employed by the Third Party to achieve risk mitigation in technical areas which do not meet PCI DSS requirements.

16 Client protection

16.1.1 The Third Party shall ensure that all Third-Party personnel (and any Subcontractor personnel) who have any face-to-face contact with members of the public in connection with the provision of Services are each issued with unique, clearly identifiable ID passes.

16.1.2 The Third Party shall ensure that such ID passes are visible on all Third-Party personnel (and any Subcontractor personnel) at all times and that a robust policy is in force to manage loss of ID cards and ID cards left at home by Third Party personnel (and any Subcontractor personnel).

16.1.3 The Third Party shall track the issue and subsequent disposal of any Campbell & Kennedy Maintenance branded items that are used in the provision of Services to Campbell & Kennedy Maintenance clients.

16.1.4 The Third Party shall maintain a written register of lost/stolen Campbell & Kennedy Maintenance branded items.

16.1.5 The Third Party shall ensure that all Third-Party personnel (and any Subcontractor personnel) do not share their unique ID number with other personnel or with any 3rd parties.

16.1.6 The Third Party shall, upon request, provide to Campbell & Kennedy Maintenance a regular list of Third-Party personnel (and any Subcontractor personnel) including details of all joiners and leavers.

16.1.7 The Third Party shall obtain all necessary licenses or permissions required in the provision of Services to Campbell & Kennedy Maintenance (e.g. trading license).

16.1.8 Where Third Party personnel (or any Subcontractor personnel) have face-to-face contact with CAMPBELL & KENNEDY MAINTENANCE clients as part of providing the Services, the Third Party shall have a policy in force detailing actions to be observed for No Cold calling zones, any by-laws and any local Neighborhood Watchschemes.

16.1.9 Where Third Party personnel (or any Subcontractor personnel) have face-to-face contact with Campbell & Kennedy Maintenance clients as part of providing the Services, the Third Party shall have in force a client interaction incident escalation process.

16.1.10 Where Third Party personnel (or any Subcontractor personnel) have face-to-face contact with Campbell & Kennedy Maintenance clients as part of providing the Services, the Third Party shall detail how any activity and geographical deployment of Third-Party staff is controlled and shall provide full details of such controls in writing if requested to Campbell & Kennedy Maintenance.

17 Documents required

17.1.1 The Third Party shall supply any of the following documents, policies and procedures upon reasonable advance request(s) by Campbell & Kennedy Maintenance:

- High-level architecture diagram
- Information Security Policy
- IT/IS Organisation Chart
- Data Retention Policy
- Data Storage and Disposal Procedure
- Security Incident Response Procedure
- Business Continuity Plan
- Data Protection Policy
- Physical Security Policy
- Acceptable Use Policy
- Disciplinary Policy

Appendix 1 – Defined Terms

The terms used here in shall have the following

"Agreement"	means the legal agreement(s) between Campbell & Kennedy Maintenance and the third party which incorporates this Security Standard by inclusion or reference
"Sensitive Data"	has the meaning set out in the Data Protection Act 1998 or equivalent
"Services"	means the services provided by the third party to Campbell & Kennedy Maintenance as set out in the supplier's legal agreement
"Sites"	means any location used by the third party in providing the services including but not limited to the supplier's sites and any other location where Campbell & Kennedy Maintenance information or materials are stored and/or processed
"CAMPBELL & KENNEDY MAINTENANCE Information"	means any and all data owned, processed or produced by or on behalf of Campbell & Kennedy Maintenance (including data produced by the third party in the provision of the services)
"CAMPBELL & KENNEDY MAINTENANCE Materials"	means any materials and/or devices supplied by Campbell & Kennedy Maintenance to the third party or otherwise generated though the provision of the services under the agreement including but not limited to all devices, computer hardware, computer and telecoms equipment, appliances, stationery, and any other materials, consumables, supplies or property of any kind
"CAMPBELL & KENNEDY MAINTENANCE Network"	means any electronic communications systems operated by CAMPBELL & KENNEDY MAINTENANCE
"Third Party"	means organisations (and their Campbell & Kennedy Maintenance approved Sub- Contractors) that provide Services to CAMPBELL & KENNEDY MAINTENANCE ion a contractual basis
"Supplier"	means organisations (and their Campbell & Kennedy Maintenance approved Sub- Contractors) that provide Services to Campbell & Kennedy Maintenance on a contractual basis
"Subcontractor"	means contractor appointed by the third party in accordance with the agreement to provide all or part of the services
"Supplier Personnel"	means any employee, contractor or agent (including the employees of such contractor or agent) of the third party engaged by the supplier to provide the services
"Systems"	means the information and communications technology system used by a party in performing the Services including any software, middleware, hardware, devices and peripheries.

Document control

Author	GK		
Document Name	Third Party Security Compliance Standard		
Version	3.0		
Source	CAMPBELL &KENNEDY MAINTENANCE Information Security		
Standard Owner(s)	IT Manager / Head of Information Security		
Date	Version	Author	Changes/Comments
01/08//2019	1.0	GK	Initial Draft, feedback and Document finalised
30/09/2021	2.0	GK	Policy review/update
27/08/2022	3.0	GK	Policy review/update
28/08/2023	4.0	GK	Policy review/update