INFORMATION SECURITY STANDARDS FOR SUPPLIERS

Moderate

PURPOSE

The IT Security Standards aims to effectively protect Computacenter, and its customers' information by providing a flexible yet consistent approach to managing information security and assist Computacenter suppliers to better understand and work co-operatively on proportionate security controls. The Computacenter Information Security Standards for Suppliers describes the minimum level of security control requirements for its Suppliers which must be met. This includes all elements involved in the provision of the Services or Goods to Computacenter or its customers.

Supplier shall reassess against the Computacenter Information Security Standards upon the earlier of (a) any material changes to any aspects of the Supplier's operations, or (b) every two years minimum.

All new Suppliers will be required to comply with the applicable (relevant to the Services and Good being delivered to Computacenter and its customers) terms of this Standards. If there is a direct conflict between any requirements of this Standard and terms of a written agreement between the Supplier and Computacenter, the terms of the written contract will prevail to the extent of the conflict.

SCOPE

The scope of this Standards includes any Suppliers that process, or have access to Computacenter's, its customers' assets, and information.

1. COMPLIANCE AND EFFECETIVENESS

Computacenter requires the Supplier to comply and evidence their commitment to information security along with the effectiveness of security measures, and such effectiveness will be reported to Computacenter upon request. These assurances will be based on information risk & security control self-assessments conducted by the Supplier.

Supplier personnel involved in the provision of Goods or Services to Computacenter, or its customers must comply with the Information Security - Acceptable Use Policy.

2. PERSONNEL (USER) MANAGEMENT

2.1. USER ACCOUNTS

Supplier Personnel may be issued with User accounts to access Computacenter Information systems and Applications. Management of such user accounts must adhere to Computacenter's Information Security - Identity, Access, and Password Policy.

- Supplier must agree a process of Computacenter registration and de-registration of their Users, both in functional roles and in administrative / privileged roles, which shall be maintained and adhered to in situations where personnel of the supplier accesses Computacenter's IT environments.

- Supplier must have a rigid process to manage Joiners/Movers/Leavers of their personnel involved in the provision of Services to Computacenter
    - Supplier Personnel Moving or Leaving their organisation, their User Accounts must be treated appropriately to minimise unauthorised access to Computacenter environment.
    - When a registered user leaves the Supplier, the Supplier shall ensure that the related user identity is blocked immediately (within one working day) and notify Computacenter Access Management about the change.
- Supplier shall conduct quarterly reviews of the list of user identities which are registered with Computacenter, and of their logical access roles and permissions, with the aim to identify any deviations, and align the review results with Computacenter.
- Supplier personnel must not use the User Account(s) provided following termination of the agreement with Computacenter, or its customers.

2.2. USE OF E-MAIL SYSTEM

Supplier Personnel may be issued with a bona fide Computacenter e-mail addresses for Computacenter business purposes and in accordance with the Computacenter's Acceptable Use Policy. Each user must read and sign the "Declaration of Commitment for Externals" before Computacenter grants access to that e-mail address.

2.3. IDENTITY CONTROL, SCREENING AND VETTING

Supplier shall comply with Computacenter's Acceptable Use Policy and additional local / service specific policies as required. Supplier shall perform the pre-engagement screening of all Personnel at the time of hiring.

Computacenter may conduct additional background checks of Supplier Personnel depending on requirements for specific positions or individual customers' requirements.

2.4. INSTRUCTIONS AND BEHAVIOUR OF SUPPLIER PERSONNEL

Supplier personnel must comply with Computacenter's Physical Access and Site Security Policies. Supplier to ensure that their service personnel (including the employees or agents of its subcontractors) do not use the Computacenter sites, equipment, or software:

- for the transmission, publication or distribution of any material which is defamatory, offensive, or abusive or of an obscene or menacing character.
- in a manner which constitutes a violation or infringement of the rights of any person, firm, or company (including but not limited to rights of copyright or confidentiality), or
- for personal purposes,

and that they are instructed to the necessary extent about the requirements flowing from Computacenter's Information Security policies and adhere to them.

Unacceptable behaviour identified whilst conducting contracted activities may lead to removal from site and individuals being reported to the Supplier Management team. A formal disciplinary process shall be followed for supplier employees who have committed a security breach.

2.5. TRAINING OF SUPPLIER PERSONNEL

Supplier ensures that all their personnel, working for Computacenter or for its customers, have undertaken a reasonable Information Security Awareness Training. Such training should be provided at the point of hiring as an Induction, and a refresher training during the length of the contract for all personnel.

3. IT EQUIPMENT MANAGEMENT

3.1. USE OF IT EQUIPMENT AND PROPERTY

Supplier Personnel may be issued with Computacenter IT Equipment or other property. For example, Two-Factor Authenticator Tokens, Photo ID Badges/Cards, Personal Computers, and Laptop computers. Removable Media (e.g. encrypted USB Drives) are prohibited from use unless an exception has been provided in writing by Computacenter. Supplier Personnel must return all items of equipment to Computacenter on request and immediately notify the Computacenter IS Service Desk if any of these items are lost or stolen. The IS Service desk can be reached 24x7x365 days per year on telephone number.

- +44 (0)1707 631111 (EN)
- +49 2273 597 7777 (DE)
- +33 148 176 99 (FR)

Should any customer equipment that has been issued to supplier personnel be lost or stolen it must be reported to the Computacenter Sponsor / point of contact immediately to ensure the situation is managed and the customer is informed. Notification should only be given to the customer by the relevant Computacenter Service Manager or point of contact.

All IT equipment provided by Computacenter (e.g. Laptop, PC, Mobile) containing Computacenter, or its customers' information must be protected against unauthorised access, misuse, or corruption during transportation beyond the supplier's physical boundary as far as reasonably practical. IT Equipment, media or information shall not be taken off the Subcontractor premises without authorisation.

3.2. USE OF NON-COMPUTACENTER OWNED IT EQUIPMENT

Non-Computacenter IT equipment (i.e. personally owned non-corporate) must not be used in the provision of Services to Computacenter, or its customers. This includes the use of private smartphones, tablets, and PDAs to replicate to and / or store information on.

3.3. REMOTE ACCESS

Should the supplier require remote access to Computacenter's IT environment, they shall.

- Only access using the specific user accounts provided to them by Computacenter,
- Only access using the Remote Access Systems[1] made available to them and must not circumvent the agreed process,
- Must only allow the designated User account for the purpose it is provided, and the purposes must be recorded in an Incident/Request/Change record,

[1] Remote Access System (RAS) includes Computacenter's Partner Citrix Farm (PCF), or CyberArk

- Must not copy (paper based, or electronically), of any information/data without explicit authorisation from Computacenter.

4. INCIDENT MANAGEMENT, REPORTING AND DISCLOSURE

Supplier personnel must report all security incidents, events, weaknesses to their point of contact in Computacenter, providing all relevant detail. Incidents, events, and weaknesses must be reported in a timely manner and no more than 24 hours after they have been identified.

Supplier shall immediately notify their point of contact within Computacenter in case of any Security Breaches which may be subject to public disclosure and other regulatory notification duties of Computacenter.

The supplier is required to inform Computacenter immediately if it suspects or is aware of any actual compromise of the confidentiality of any Computacenter User Account details that they have been provided.

APPENDIX

Computacenter relevant Security Policies are listed below. The Supplier will be provided with the relevant policies, as necessary.

- Information Security – Acceptable Use Policy
- Information Security - Identity, Access, and Password Policy
- Physical Access and Site Security Policy