INFORMATION SECURITY STANDARDS FOR SUPPLIERS

SUBSTANTIAL

Purpose 2
Scope 2
1. Information Security Governance 2
2. Compliance and effectiveness 2
3. Outsourcing of services to third or fourth parties 3
4. Information Security Risk Mitigation 3
5. Identify Control, Security Clearance, Screening and Vetting 3
6. Personnel Training 3
7. Security Audit 4
8. Procurement, Development & Maintenance of IT Systems and Software 4
8.1. Software Services 4
8.2. Remote Access 4
8.3. Information Exchange Requirements 5
8.4. Supplier Usage of “Cloud-Based” Services for Processing Information 5
8.5. Supplier IT Infrastructure Security 6
8.5.1. Segregation of multi-tenant infrastructure and applications 6
8.5.2. Separation of Production, Test and Development Environments 6
8.5.3. Availability Management; Backup Management 6
8.5.4. Asset & Configuration Management 7
8.5.5. Operations Monitoring, Log & Event Management 7
8.5.6. Change & Release Management 7
8.5.7. Vulnerability, Patch Management and Penetration Tests 7
9. User Accounts Management 7
9.1. Registration and de-registration & User access review 7
9.2. Roles based logical access control, privileges, and provisioning 8
9.3. Secure log-in procedures 8
10. Mobile Device management 8
11. Incident Management, reporting and disclosure 8
12. Protection Against MAlware 9
13. Data Encryption & Cryptography Management 9
14. Business Continuity Management & Disaster Recovery Planning 9
15. Contract Termination; Return of Information & Processing Assets 10
Appendix A 10

PURPOSE

The Information security standards are designed to effectively protect Computacenter and its customers' data by providing a flexible yet consistent approach to managing data security and helping Computacenter providers better understand the relevant security controls and to work with Computacenter on these controls. Computacenter's Information security standards for vendors describe the minimum-security control requirements that vendors must meet. They cover all aspects relevant to the provision of services to Computacenter or its customers.

Providers must review Computacenter's Information security standards as soon as (a) significant changes in the provider's operations come into effect or (b) at least every two years.

All new providers are required to comply with the applicable terms of these standards which relate to the provision of services to Computacenter and its customers. If there is a direct conflict between the requirements of these standards and the terms and conditions of a written agreement between the provider and Computacenter, the terms and conditions of the written agreement shall prevail to the extent that they relate to the conflict.

SCOPE

The scope of this Standards includes any Suppliers that process, or have access to Computacenter's, or its customers' assets and information. This includes, but not limited to:

- Suppliers that process, access, hold or transmit information for Computacenter and its customers.
- Access to Computacenter environment from remote locations where the IT facilities are not under the control of Computacenter.
- Supplier personnel that require access to Computacenter or its customers' information, or all elements of IT systems.
    - This Standard, therefore, also applies to all personnel including contractors, temporary employees, and supplier employed directly, or indirectly by the Supplier.

1. INFORMATION SECURITY GOVERNANCE

The Supplier shall ensure:

- that they have appointed personnel who has overall responsibility for the organisation's information security programme and their organisations ongoing compliance to the Computacenter's Information Security Standards
- that the information security policies of their organisation are produced, approved, reviewed annually, and communicated to all personnel.
- that they have an information assurance governance that is actively used to monitor and report the effectiveness of security arrangements to the Supplier governing body

2. COMPLIANCE AND EFFECTIVENESS

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 carried out by the Supplier.

- As a minimum all supplier personnel, involved to provide services to Computacenter or its customers or who get access to its information, or to Computacenter's site(s) must.
    - Implement general information security best practices across all supplied components and materials including software, hardware, and information to safeguard the confidentiality, availability, and integrity of Computacenter and its customer information,

- read, understand, and comply with Computacenter's Acceptable Use Policy,
- classify and handle any protected information bearing assets according to the requirements of information classification and handling as specified by Computacenter policies,

Should there be a requirement for the Suppliers to comply with specific Customer Security Policies, Computacenter will issue relevant policies to the Supplier.

3. OUTSOURCING OF SERVICES TO THIRD OR FOURTH PARTIES

The Supplier is not authorised to outsource in whole, or in part, services which are covered by the contract to third or fourth parties without prior written consent by Computacenter. Where Computacenter has agreed that specific activities are subcontracted by the Supplier, the subcontractor must not be entitled for further outsourcing without prior consent by Computacenter.

Supplier shall ensure (as part of its Information Security Management approach) that the underpinning supply chain is controlled, and the security compliance requirements of an agreement are enforced along the supplier's supply chain. Evidence of security compliance assessments conducted for any 3rd party services where Computacenter information or data is stored or processed, including any available 3rd party independent security assessment reports must be provided to Computacenter on request e. g. ISO27001 Accreditation, SOC-2 reports.

4. INFORMATION SECURITY RISK MITIGATION

Supplier shall operate an Information Security Risk management approach that is appropriate to identify any risks, that are caused by its IT services, to the Information Security of Computacenter. Supplier shall comprehensively document and assess the identified risks and provide mitigating safeguards.

Based on that, Supplier shall, in collaboration with Computacenter, maintain a security plan containing the risk mitigation safeguard specifications, and the effectiveness status of these safeguards, with respect to the identified risks to the Information Security of Computacenter. The Supplier will provide such Risk Logs to Computacenter containing of the Risks raised concerning the Security of Computacenter, and its customers within the provision of the goods and services agreed upon request within a reasonable timeframe.

5. IDENTIFY CONTROL, SECURITY CLEARANCE, SCREENING AND VETTING

Supplier shall ensure that any Supplier Personnel who will have:

- Physical access to any Computacenter Site(s),
- Remote Access to Computacenter, or its customers data,

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.

6. PERSONNEL TRAINING

In the provision of Services to Computacenter or its customers, the Supplier will ensure that.

- Security awareness training forms part of the compulsory induction and training programme for all their new or existing personnel
- all personnel are aware of information security threats and concerns, their responsibilities, and liabilities, and are equipped to support organisational security policies.
- review such training and briefing requirement on a regular basis.

Computacenter may require its Supplier to provide a report on the status of the training being provided to its personnel participating in the provision of services to Computacenter and its customers.

7. SECURITY AUDIT

Computacenter shall be entitled, upon reasonable notice, to conduct Information Security Audit to assess Supplier compliance to the Agreement and services being provisioned at the location of the supplier by Computacenter or by an agreed external audit provider. Audits will be carried out at agreed times and with an agreed scope. Compliance with contractual and service requirements will be checked in the context of an audit. Audit findings shall be verified and tracked with the Supplier.

In case of any deviation or non-conformities found during information risk & security self-assessments, or during the audits of the Supplier services, the supplier will ensure that appropriate risk mitigation and corrective action plans are implemented in a timely manner, and accomplishments reported to Computacenter.

8. PROCUREMENT, DEVELOPMENT & MAINTENANCE OF IT SYSTEMS AND SOFTWARE

8.1. SOFTWARE SERVICES

For the provision of Software related Services to Computacenter or its customers, the Supplier.

- shall consider that the software does not include known flaws, for example, described in the latest version of "OWASP[1] (Open Web Application Security Project) Top Ten most critical Web application vulnerabilities as a minimum.
- shall endeavour to adopt best practices from OWASP (e.g. OWASP Testing Guidelines, OWASP Maturity Models)
- has adopted the industry recognised processes such as SDLC (Software Development Life Cycle) to ensure that both usability and warranty are ensured.
- warrants that any provided / utilised software will not contain any malicious code (including computer viruses, worms, logic bombs, Back-doors and Trojans and any other form of malicious code) that weakens the security of the application.
- ensures that they will only ever supply software that can be independently verified as fit for purpose and does not contain any commonly known weaknesses or vulnerabilities.
- ensures that any code (including any 3rd party code) will be tested before launched into Production environment, and a local copy is taken rather than referencing to it as a separate assembly.
- will disclose, upon request from Computacenter, all Third-Party Software used, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed source
- will also provide timely details on any end-of-life product(s) or service, along with any upgrade options allowing Computacenter to assess any security risk and viable options to mitigate any risks.

The Supplier agrees to provide reasonable support to Computacenter Review Team by providing source code. Supplier will provide software escrow arrangements for the source code where the software source code is not being delivered to Computacenter as part of the agreement.

8.2. REMOTE ACCESS

The Supplier, should they require to have remote access to Computacenter's IT environment(s), will comply with the following standards for the provision of the Services or Goods to Computacenter.

- Supplier must only access Computacenter IT environment(s) using Remote Access System[2] which must only be used for the purpose of fulfilling the contractual obligations for the provision of the Goods and Services being provided to Computacenter,
- Suppliers must implement security measures to protect their IT environments from any security risks (including vulnerabilities, security threats, malware viruses) associated with using such a Remote Access solution[2],
- Supplier must have implemented and operate appropriate security controls (technical, procedural, and organisational) to prevent unauthorised use and positively identify all users of their IT Infrastructure at their premises in accordance with Computacenter's Identity, Access, and Password Policies,
- Usage is permitted only for a valid support Incident, or for an approved Change Request which must be formally logged by Computacenter and on Supplier's Support Systems[3],
- Supplier must treat information according to the Information Classification and Handling Matrix when sharing screen (e.g. Microsoft Teams sessions) with Computacenter employee,

[1] Open Web Application Security Project Top Ten Security Risks are available on the World Wide Web

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

[3] Supplier Support System includes Service Desk Tools to manage Incidents/Changes/Requests.

- Supplier shall be accountable for all actions performed using such user account on Computacenter's IT environments.
- Supplier personnel, or owner of the Assets, should obtain authorisation to install software required to be able to access Computacenter's Remote Access System[2]. Computacenter do not own, provide a license, or support of the software required to access their Remote Access System[2],
- Computacenter reserves the right to disable or suspend the Supplier's use of the Remote Access System[2] solution for any reason without notice. Computacenter acknowledges that if the Supplier is not able to use Remote Access Solution[2] as a result of suspension or disablement then any applicable Service Levels shall not apply for the period that it is unable to use the RAS[2] solution,
- The RAS[2] solution can be used to transfer data to or from the Computacenter's IT Infrastructure. Supplier Personnel are prohibited from making copies of any Computacenter or its customer data that is stored on any Computacenter IT system and / or transfer such data to the Supplier's device, or any other storage location outside of the Computacenter IT Infrastructure without specific written approval from Computacenter,
- Access or Usage of the Computacenter's Remote Access System[2] will cease on termination of an Agreement with the Supplier.

8.3. INFORMATION EXCHANGE REQUIREMENTS

- Suppliers shall always maintain management-approved corporate Information Security Policy, or a set of Security Policies, defining responsibilities and approach to Information Security.
- Computacenter, or its customer's Information is classified in accordance with the criteria defined within the Computacenter's Acceptable Use Policy (chapter: Information Classification & Handling / Information Classification & Handling Matrix). Classification drives the requirement for the protection of the Information when it is transmitted and stored electronically.
- Computacenter and the Supplier have agreed the most appropriate method of electronic information exchange for the provision of Goods or Services to Computacenter or its customers.
- The Supplier must not copy (paper based, or electronic), of any Computacenter, or its customer information/data without explicit authorisation from Computacenter,
    - such authorisation to proceed must be recorded in an Information Transfer Log

Note that exchanges of ad-hoc and general business communication are excluded from this definition.

8.4. SUPPLIER USAGE OF "CLOUD-BASED" SERVICES FOR PROCESSING INFORMATION

- Storage and processing of Computacenter Information by Supplier using 3rd party Cloud Based Technology Delivery Platforms (i.e. Infrastructure-as-a-service, Platform-as-a-service, and Software-as-a-service) must be compliant with the Security requirements described in this document.
- Suppliers providing Cloud Service must provide a process for data destruction and secure deletion of any Computacenter data as needed. This includes a process for sanitization ("zeroing out") of storage containers and removal of ephemeral data.
- Suppliers providing Cloud Services must have an established method of encrypting sensitive data in storage and in transit following industry best practices.
- Suppliers providing Cloud Service must securely handle Computacenter, or its customers data and assets by providing logical isolation and secure migration.
- Suppliers providing Cloud Service must include methods or options for multi-factor authentication for cloud administrator roles and as required by Computacenter or its customers. Furthermore, Computacenter expects the Cloud service provider to implement best practices such as Multi-factor authentication for control of access to the service provider's infrastructure management systems.
- Suppliers must comply to Computacenter's Identity, Access and Password Policies and Acceptable Use Policies.
- Suppliers providing Cloud Service must have documented audits or established compliance roadmaps in alignment with Industry Standard Certifications for Cloud Security (examples include ISO270017, NIST.SP.800-144, Cloud Computing Compliance Controls Catalogue (C5), CSA STAR, SSAE16, FEDRAMP, FIPS 140-2, and Open Data Alliance)
- Cloud based services must demonstrate how they achieve BC/DR[4] requirements.
- Supplier must disclose if information is being processed outside of the EEA.

[4] BC/DR = Business Continuity / Disaster Recovery

8.5. SUPPLIER IT INFRASTRUCTURE SECURITY

Suppliers are to comply with Computacenter Security Standards in relation to their Infrastructure that is incorporated in the provision of the Goods and Services to Computacenter.

- Supplier must support standards and procedures that ensure confidentiality, integrity and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented Risk Assessment process driving risk mitigation implementation on a timely basis.
- Suppliers must maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed, or managed through processes such as Change Management, Vulnerability/Threat Management, and Information Security Incident Management
- Supplier must define the end-of-life process (EOL) for all components of the infrastructure which could include date of EOL and any business triggers that may result in updated EOL date.
- All sensitive Personal Identifiable Information (PII) transferred must be properly secured. System must not transfer PII to other systems or be used for purposes other than specified, unless approved by Computacenter or the individuals the information belongs to.
- Network segments connected to the Internet must be protected by a firewall which is configured to secure all devices behind it addressing all known security concerns.
- Applications, ports, services, and similar access points installed on a computer or infrastructure facility, which are not specifically required for the provision of Services to Computacenter, must be disabled or removed.
- All extranet connectivity into Computacenter must be through Computacenter approved and authorized secure remote connections.
- Supplier is responsible for implementing the secure protocols at their sites and managing the protocols by a Change Control process.
- Systems must have the ability to detect a potential hostile attack. Examples include, but are not limited to, Network Intrusion Detection (NID) or Host Intrusion Detection (HID) / Prevention. All systems must be updated to current release and actively monitored.
- Infrastructure diagrams, documentation and configurations must be up to date, controlled and available to assist in issue resolution.

8.5.1. SEGREGATION OF MULTI-TENANT INFRASTRUCTURE AND APPLICATIONS

Computacenter understands that the Supplier may provide Services to multiple customers, and therefore, through appropriate technological and organisations means, the following standards must be adhered to.

- Logical segregation of IT systems and Applications in which the Services are performed for Computacenter.
- Any virtual environments that Computacenter Services are being provided from, shall be protected from other customers of the Supplier through strict access controls.
- Data shall be separated on the technology architecture level in accordance with data security architecture requirements.
- All elements (including facilities, and technical infrastructure) required to provide the Services to Computacenter are kept reasonably separated (physically, or logically) from the Supplier's other customers.

8.5.2. SEPARATION OF PRODUCTION, TEST AND DEVELOPMENT ENVIRONMENTS

- Supplier shall ensure that during development and maintenance of any contracted services, the production, test and development environments, and production and test data are separated (logically or physically)
- Acceptable criteria for new information systems, upgrades and new versions must be established and suitable tests of the system(s) carried out during development and prior acceptance and implementation into Production environment.
- Access rights are controlled through appropriate groupings and associated rights management to ensure logical data separation between customers.

8.5.3. AVAILABILITY MANAGEMENT; BACKUP MANAGEMENT

- Supplier shall implement an Availability Management process appropriate to comply with the agreed Service Levels / Security Service Levels for the specific Services being delivered to Computacenter, or its customers.
- To ensure availability in any emergency, and after major incidents / outages, appropriate Backup Management shall be implemented, and Recovery Management planned and tested.

8.5.4. ASSET & CONFIGURATION MANAGEMENT

- An Asset register must be established and maintained for the purposes of the contracted service with Computacenter.
- Supplier ensures that these information assets are not shared with others unless this agrees with Computacenter process to deliver the contracted services.
- Any assets utilised in the provision of Services to Computacenter should be stored securely and must be protected against unauthorized access, disclosure, modification, destruction, or interference.
- Any Computacenter or its customers information must be deleted from the devices before being reused for any other purposes.

8.5.5. OPERATIONS MONITORING, LOG & EVENT MANAGEMENT

- An automatic event reporting system should be available.
- Audit logs recording user activities, exceptions, and information security events must be maintained for an agreed period to assist in the investigations and access control monitoring.
- Technical controls must be in place for system monitoring to collect security system events.
- Security-related event logs from any components in the infrastructure must be reviewed and acted upon
- Supplier must have an Event Management process implemented that is documented and operationally assessed to detect cyber threats against the provided solutions and services.

8.5.6. CHANGE & RELEASE MANAGEMENT

- Supplier shall ensure that all changes to contracted services (including and not limited to Business Process Changes, IT Service Changes, Application/ Platform/Infrastructure Changes, or changes to underlying physical and technical premises) are controllably processed through a formal Change Management Process.
- Where changes affect the contracted services, all changes are subject to prior announcement and approval by Computacenter.
- Any release of changed services and solutions may only take place based on an approved Change Request and based on a formal Release Management Process of the supplier.
- Any online software provision, or automated software distribution by the supplier must adhere to Computacenter's Information Security Policies

8.5.7. VULNERABILITY, PATCH MANAGEMENT AND PENETRATION TESTS

Supplier shall have effective Vulnerability and Patch Management Processes implemented to reduce risks resulting from exploitation of published technical vulnerabilities. Supplier must comply with Computacenter's Technical Vulnerability Management Policy.

9. USER ACCOUNTS MANAGEMENT

9.1. REGISTRATION AND DE-REGISTRATION & USER ACCESS REVIEW

Suppliers will manage Supplier's Personnel User Accounts in accordance with Computacenter's Identity, Access and Password Policies, and Acceptable Use Policies. In specific and not limited the following.

- 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 1 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.

9.2. ROLES BASED LOGICAL ACCESS CONTROL, PRIVILEGES, AND PROVISIONING

As part of the service specification, a roles and responsibilities plan will be agreed. The roles will be specified in a way that access is restricted to the business needs. Administrative roles with privileged access will also be specified and agreed.

- Supplier will document the privileged roles which are be implemented for the Supplier's personnel to access Computacenter's information assets.
- A logging concept for all privileged access will be provided by the Supplier, and these admin logs will be made available for Computacenter on request.
- For Cloud Services, the Cloud Supplier will specify the access control requirements to the Cloud IT environment.
- Supplier shall ensure enforced control of all privileged access and log management of all privileged activities on operations systems, database, middleware, and business application level. Activities using privileged access shall be controlled by appropriate Log Management.

9.3. SECURE LOG-IN PROCEDURES

Supplier shall ensure secure login processes, including Use of recognised industry standards for the authentication and authorisation (e. g. multi-factor authentication, no use of jointly used authentication information, automatic expiry) for all accounts (standard or privilege accounts)

10. MOBILE DEVICE MANAGEMENT

- The supplier 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 in the provision of Services to Computacenter or its customers.
- The supplier and its personnel must adhere to the applicable Computacenter Information Security Policies

11. INCIDENT MANAGEMENT, REPORTING AND DISCLOSURE

- Supplier shall always maintain Incident Management Processes and Procedures that includes steps to manage Major Incidents, or Security Incidents
- A documented Incident management process for Physical and Data security must be implemented which includes incident response, functional or hierarchical escalation, and remediation.
- 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 at the earliest opportunity 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.
- Information security events and incidents include:
    - loss of service, equipment, or facilities,
    - system malfunctions or overloads,
    - human errors,
    - non-compliances with policies or guidelines,
    - breaches of physical security arrangements,
    - uncontrolled system changes,
    - malfunctions of software or hardware,
    - access violations,
    - legal and regulatory violations
    - Malware
    - Suspicious and benign behaviours that may lead to an event.
- Supplier must agree and implement reporting procedures for all relevant Major & Security Incidents to Computacenter should the contracted service agreement, and their security compliance level may be affected.

- Supplier shall report on the results, and initiated Changes to treat any detected flaws or vulnerabilities, on a timely manner after resolution of any major & security incidents affecting the provided services.
- Both companies will act in good faith to preserve the other company's evidence and reasonably cooperate with each other and the authorities if needed during an investigation.

12. PROTECTION AGAINST MALWARE

- The Supplier shall have anti-virus solution implemented on all Supplier's systems vulnerable to virus infection.
- The Third Party 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 Computacenter Information; or
    - disabling or locking any software or Supplier Systems or Computacenter Systems; or
    - using undocumented or unauthorised access methods for gaining access to Computacenter Information, or Supplier or Computacenter IT Systems.
- The Supplier shall ensure that the malware protection tool deployed:
    - is a current and supported version.
    - is updated with definition or signature files daily as a minimum.
    - provides real time on-access and on-demand scanning.
    - scan all content entering and leaving the IT infrastructure processing Computacenter Information.
    - can disinfect, quarantine, or delete malware.
    - can provide logging, alerts, and reporting functionality; and
    - cannot be disabled, reconfigured, or prevented from working by unauthorised users.
- The supplier shall ensure that anti-virus software and anti-virus definition files are updated for all Supplier Systems in line with best business practice and in accordance with advice from applicable anti-virus software.
- Supplier must ensure devices can detect, isolate, and defeat malicious code which is present on devices.

13. DATA ENCRYPTION & CRYPTOGRAPHY MANAGEMENT

The aims of using cryptographic controls (encryption, digital certificates, digital signatures) are to ensure data confidentiality (to prevent unauthorised disclosure), to preserve the integrity of data (by preventing or detecting unauthorised modification), and authenticity and non-repudiation (by proving that the sender of the information is who they claim to be).

- Supplier shall ensure effective data encryption for information residing on systems while at rest. Encryption must be used for data in transit containing personal or sensitive information or any other confidential information as specified by Computacenter.
- Transmission medium must not be used If it does not offer sufficient level of protection unless it has been authorised by Computacenter's Information Security Management
- Supplier must plan for a thorough end-to-end Key Management process that will include secure key generation, use, storage, and destruction.
    - Considerations need be made as to how these key management practices can support the recovery of encrypted data if a key is inadvertently disclosed, destroyed, or becomes unavailable.
    - The supplier needs to ensure that access to encryption keys is secured, and only available to authorised personnel. The keys themselves should be physically secured with at least two upper-level trustees' assigned access.

14. BUSINESS CONTINUITY MANAGEMENT & DISASTER RECOVERY PLANNING

In provision of the Services to Computacenter, or its customers, the Suppler must comply to the below standards in terms of Business Continuity (BC), and Disaster Recovery (DR).

- Supplier covenants to participate in the creation and maintenance of an ICT emergency plan based on Standards ISO 22301 and ISO 27031. The first version of the emergency plan, together with any updates, shall be submitted to Computacenter for co-ordination by the responsible service manager (contact person) of the Supplier, and its validity shall be predicated on the express, written approval of Computacenter.
- Supplier shall ensure Business Continuity/Disaster Recovery Management plans, approved by their Senior Management, inclusive of technical and non-technical components, exist and updated.
- The BC/DR plans must provide transparent indication of the workaround, and total restoration times to restore the Services being provided to Computacenter, or its customers.
- Supplier must have established communication channels with Computacenter during the BC/DR period.

- All Supplier personnel involved in the provision of the Service must be aware of the BC/DR plans and their responsibilities during the BC/DR period.
- All Computacenter data has a regularly scheduled backup and restore capability implemented and tested.
- Disaster recovery resources and / or Supplier's must be documented and made available to Computacenter upon request.
- Supplier also covenants to participate actively in the emergency activities of Computacenter where necessary, which may include business-continuity and recovery plans.

15. CONTRACT TERMINATION; RETURN OF INFORMATION & PROCESSING ASSETS

Upon the termination of the Service Agreement between the Supplier and Computacenter, the following must be adhered to.

- Computacenter and the supplier must agree an Exit Management plan on a timely basis,
- The Exit Management Plans shall include the end of Service being provided to Computacenter, including Cloud-Based Services, and/or transfer to Computacenter selected supplier in an agreed format.
- Supplier must return of all assets which are the property of Computacenter, and secure destruction of information from the supplier's environment, as specified in the Exit Management Plan

APPENDIX A

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

- Acceptable Use Policy
- Identity, Access & Password Management Policy
- Technical Vulnerability Management Policy
- Malware Prevention Policy
- Network Security Policy
- Software Security Policy
- Endpoint Security
- IT Data Security Policy
- IT Security Architecture Policy
- IT Service Continuity Management Policy
- IT Monitoring and Event Logging Policy
- Technical IT-Infrastructure (Secure Areas) Policy
- Physical Access and Site Security Policy