

TELEFÓNICA O2 UK LTD

SECURITY POLICY

TELEFÓNICA O2 UK SECURITY POLICY

1. Overriding Principles

O2 attaches particular importance to the security of its own, its employees' and its customers' data. It is therefore vital that existing and potential new suppliers to O2 have appropriate security controls to ensure the confidentiality, integrity and appropriate availability of such data is not compromised and these controls are maintained in accordance with O2's security policies.

The reference standard for O2's security policies is ISO27001 and the Supplier shall comply with the principles of that standard at all times.

2. Introduction

The O2 security policies form two parts:

1. this short form summary of the key principles of the policy which lists the baseline security requirements which should be incorporated into systems required to protect O2 customer or other O2 related business data; and
2. the full O2 security policy set which is managed by the O2 Fraud & Security team on behalf of the Telefónica O2 Europe Group of companies.

Each Supplier must comply with both these policies, together which are known for the purpose of this Agreement as the "O2 Security Policy".

It is the Supplier's obligation to request the most recent copy of the O2 Security Policy from O2's Fraud & Security Department by contacting O2.

If the Supplier is not already a party to an NDA with O2 that would cover this situation, O2 may ask Supplier to enter into such an NDA with O2 specifically in respect of this O2 Security Policy. Failure to request a copy of the O2 Security Policy will not absolve Supplier of its obligation to comply with it. Any variations to Supplier's compliance with the O2 Security Policy must be recorded in writing and must be signed by both parties.

Suppliers must have their own defined security policy, which must be supported by documented security requirements and procedures and which mirrors in all material respects the O2 Security Policy.

The Supplier's management (Board level directors or equivalent) will:

- Demonstrate that information protection is a critical business issue.
- Assume ultimate responsibility for information security.
- Be directly involved in creating a security culture across their business.
- Ensure the company's security objectives and policy is available to all employees.
- Allocate sufficient resources to information security.
- Ensure personnel policies and contracts and contractor non-disclosure agreements reflect the requirements of the security policy.

3. Security Controls

The remainder of this document lists various high level security controls and objectives, which O2 require their suppliers to comply with at all times.

Any following reference to 'data' will be to O2 customer, business and other sensitive data or information.

3.1. Access

3.1.1 General provisions

- Access to the data must only be available to people who are authorised.
- Before any data is made available to any 3rd party supplier or non-O2 business partner Supplier must arrange for a non-disclosure or confidentiality agreement to be agreed and signed between O2 and such 3rd party supplier or non-O2 business partner.

- The risks to data must be identified by Supplier and appropriate controls implemented within Supplier systems before access to data. These controls will include physical, technical, process and people protection arrangements to provide layers of defence to prevent the unauthorised disclosure, modification, deletion or other misuse of data.
- Data access must use unique user accounts with appropriate identification and authentication controls.
- Protection of portable media used to store data must be in accordance with access control principles and must include appropriate labelling and encryption.
- Background verification checks on all existing employees, candidates for employment, contractors, sub-contractors, agency workers, third party users (and any like persons) should be carried out in accordance with relevant laws, regulations and ethics, and proportional to business requirements, the classification of the information to be accessed, and the perceived risks.

3.1.2 Grant of Access

A. If necessary for the purposes of the provision of Services under this Agreement, O2 may grant individual employees of Supplier access to its IT and/or mobile telephony networks (the “**Network**”) whether remotely, or on-site (in either case a “**Grant of Access**”). If a Grant of Access is granted, the following conditions shall apply to its use:

- O2 may withdraw the Grant of Access at any time without giving a reason;
- O2 may monitor any or all use of the Grant of Access;
- O2 may stipulate from time to time conditions on use which may cover, without limitation, security checking (see below) and restrictions on use;
- Supplier shall use the Grant of Access strictly for the purposes of the Agreement; and
- In respect of any malicious, illegal or unauthorised use of the Grant of Access by its employees or agents, Supplier shall be fully responsible at law.

B. Prior to permitting any person to use the Grant of Access, Supplier shall (and shall confirm such compliance in writing to O2):

- procure that such person is bound by appropriately strict terms as to confidentiality;
- perform a thorough background check on such person, and ensure that such person has not been convicted of any criminal offence (other than minor motoring offences) for a period of 10 years prior to the date of such background check; and
- ensure that such person has an appropriate and valid security clearance.

C. If relevant, Supplier undertakes to abide by, and ensure that its agents and staff abide by the provisions of the Official Secrets Acts 1911 to 1989 during the continuance of the Agreement and indefinitely after its expiry or termination.

D. The provisions relating to the Grant of Access are material to the Agreement and breach will allow O2 to terminate the Agreement.

E. If, in the course of using the Grant of Access, and whether by act or omission Supplier (and/or any of its staff or agents) causes any damage to the Network, including, but not limited to (i) physical damage to equipment and/or (ii) the introduction of any virus, or any other damage to systems, code or software or firmware and/or (iii) the interruption of Network service, then Supplier shall indemnify O2 and hold it harmless in respect of all losses (including losses of revenue), costs, claims, expenses, liabilities or duties whether civil or criminal. The indemnity provided under this clause shall not be subject to any exclusion or limit on liability set out elsewhere in this Agreement.

3.2. Accountability

- All accesses to data must be accountable to an identified person or machine process.
- Processes must exist to authorise, modify and remove access to data. All such changes must be recorded.

- All equipment used to process data shall be maintained using a reputable company in accordance with required security controls.
- Where there is a need to dispose of magnetic media it must be disposed of securely and safely.

3.3. Audit

- Access to key O2 systems, processes, data and buildings must be recorded in an audit log, which can only be viewed by a limited number of authorised people and maintained for an agreed period.

3.4. Business Continuity

- Adequate business continuity planning should be put in place to protect the key services that you are providing to us under the Agreement. Business continuity plans should provide appropriate protection for the defined availability as set out in the service level agreement (if applicable). The validity of a business continuity plan should be regularly rehearsed to ensure that it remains suitable, fit for purpose and current in the then current technical and physical environment.

3.5. Validation & Integrity

- Data input must be verified to ensure that its validity and integrity is correct.
- A formal change management process must exist to ensure that changes to information processing facilities and systems are controlled.
- Acceptance criteria for new information systems, upgrades, and new versions must be established with O2 and suitable tests of the system(s) carried out during development and prior to acceptance. It is Supplier's responsibility to arrange this.
- An appropriate system security patch management regime, with regular updates, must be implemented to ensure ongoing system integrity when new security vulnerabilities are discovered.

3.6. Malicious Software

- Detection, prevention and recovery controls to protect against malicious code (e.g. viruses) and appropriate user awareness procedures must be implemented and maintained.

3.7. Duty & Responsibilities

- All people dealing with O2 data or information should ensure that they are familiar with the O2 Security Policy and comply.
- Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organisation's information security policy.
- A documented security escalation process must exist and be maintained.
- Users of information systems and services are required to note and report, through the escalation process, any observed or suspected security weaknesses in systems or services.

3.8. Legal Responsibilities

- All software used by the Supplier to discharge its obligations under the Agreement must be validly owned or licensed by Supplier; it is Supplier's responsibility to maintain this.
- The provisions of the Data Protection Act 1998, PCI Data Security Standard, Sarbanes-Oxley Act of 2002 and other relevant legislation, regulation and contractual obligations must be fully complied with.
- All relevant statutory and regulatory requirements and the Supplier's approach to meet these requirements must be explicitly defined, documented, and kept up to date for each information system and the organisation.
- As part of their contractual obligations, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organisation's responsibilities for information security.
- A prescribed warning screen shall be displayed immediately after a user successfully completes the logon sequence. The system administrator shall set up procedures to provide written authorisation to users stating their access privileges.

3.9. Network Interconnection

- Networks must be adequately managed and controlled, in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit.
- Any system used to process data must not be connected to other non-trusted networks without adequate security protection mechanisms. This requirement includes communication links that are used for remote diagnostic purposes, etc.

3.10. System/Data Segregation

- Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of O2's assets.
- Data should be available on a 'need to know' basis. It must not be possible for users or customers (whether external or internal) to gain access to data that is not relevant to them.
- Development, test and operational facilities must be separated to reduce the risks of unauthorised access or changes to the operational system.

3.11. Training & Education

- Adequate security training and education must be provided to all people before they are provided with access to data or information.

3.12. Ownership

- All systems/processes/data must have a nominated owner / person responsible.

3.13. Fraud identification, detection and prevention

- Where relevant, appropriate mechanisms must be implemented and maintained to prevent and/or detect potential fraud.

3.14. Back-up/Archive

- Appropriate backup and storage for system/data must be provided to ensure that an asset can be restored.
- Copies of the current versions of the system software, data and accompanying documentation must be safely stored and available so as to enable a quick and controlled recovery in case of a processing interruption.

3.15. Non-Repudiation

- Where relevant, adequate controls should be put in place to ensure that actions and events will have legal effect and cannot be challenged in this respect and cannot be denied by Supplier and that such actions are accountable to a particular individual within Supplier organisation.

3.16. Regular Review

- Regular reviews (at least annually) should be undertaken to ensure that the security of assets cannot be compromised.

3.17. Right of Audit

- Notwithstanding anything in any agreement you have entered into with O2, in respect of security reviews, O2 shall have the right throughout the term of it agreement with you to undertake a security review at an agreed and convenient time to ensure that data has the appropriate level of security protection. This security protection will include measures relating to technical, physical, procedural and people measures and controls.