Vodafone Supplier Security Schedule

Owner:	Version:	Date:
Group Corporate Security & Group Cyber Security	Version 1	1st May 2025

Table of Contents

1 PURPOSE
2 DEFINITIONS
3 SECURITY PRINCIPLES
RIGHT TO AUDIT
4 SECURITY OPERATIONAL MANAGEMENT
4.1 Incident Management
4.2 Supplier & External Fourth Party Security
4.3 Supplier Management
4.4 Termination and change of contract
5 SECURITY CORE CONTROLS
5.1 Organisational Measures - Corporate Security
5.1.1 Personnel and Physical Security
5.1.2 Business Continuity Management
5.1.3 Fraud & Investigations
5.2 Technical Measures - Cyber Security
5.2.1 Information Asset classification, handling and protection
5.2.2 Security Hygiene
5.2.3 Identity & Access Management
5.2.4 Software Development
5.2.5 Network Security
5.2.6 Security Logging & Monitoring
ANNEX 1 - VULNERABILITY AND ISSUE FIXING TIMELINES

Purpose

At Vodafone security is part of our core purpose, and it underpins customer trust. We prioritise Cyber Security and Corporate Security across all parts of our company and with the partners we work with. Supplier should use a threat led approach to reduce risks across all activities.

Our suppliers and partners should always adopt Vodafone's security requirements as set out in this schedule, relevant to the scope of work being undertaken. The Supplier is responsible for the ongoing compliance with these requirements and to identify and action any acts or areas of non-compliance. These requirements will apply to all people, premises, telecommunications, technology infrastructure, equipment and assets and information facilities, (including contractors, temporary employees and third parties employed either directly, or indirectly by the Supplier).

Definitions

In this document, the following words and expressions shall have the following meanings:

Term	Definition
Agreement	means the underlying contract
4th party	means the Supplier's contractors and their subcontractors (of any tier)
Authorised User	means personnel employed by the Supplier who have a legitimate need and are authorized to access Vodafone Information and Systems or carry out any processing of Vodafone Information
Data Record	means any information (in whatever form) created or received, and maintained as evidence and as an asset by the company, in pursuit of legal obligations or in the transaction of business
Fraud	means any intentional, dishonest act committed for gain. Dishonesty means unlawful, unethical behaviour which often involves deception. Gain in this context refers to any unfair advantage pursued by the perpetrator, from obtaining money and property to altering a company's books to get better loan conditions or avoiding loss of one's job
Incident Response	means actions taken to mitigate or resolve a security incident, including those taken to protect and restore the normal operational conditions of a system and the information stored in it
Security Incident	means any event which causes a disruption in the provision of the contractual service(s) and/or an actual impact to the confidentiality, integrity or availability of Vodafone systems, services, the stored or transmitted or processed Vodafone Information.
Systems	means the software, hardware, servers, hosting facilities, information systems used to access, store, or otherwise process Vodafone Information, including temporary files, including telecommunication systems and other technology infrastructure and assets.
Media	means hard-copy (paper) and electronic storage media on which data is recorded and stored or from which data may be retrieved.
Products and Services	means the products and services provided by the Supplier under the Agreement
Security Breach	means the accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Vodafone Information or Systems
User Identity	means the personal and unique identifier issued to every Authorised User
Vodafone Information	means any information that the Supplier processes, creates or otherwise has access to on behalf of Vodafone in connection with providing the Products or Services, including any Personal Data and Confidential Information

Terms not defined in this Schedule shall have their meaning set out in the Agreement.

3.1 Security Principles

Supplier shall meet all security requirements in this schedule, protect all data records and regularly review security processes including

a) meet and comply with all requirements in this Schedule and any additional security annexes agreed between the parties, as applicable.

b) maintain independent evidence of the status of its security controls (e.g., ISO27001, ISO22301, SOC2 or Cyber Essentials Plus) and provide a copy to Vodafone upon request.

c) use multi-factor authentication and VPN across all devices which can be used to access services, systems, and networks from the Internet as well as for the Internet facing services.

d) utilise and enforce a process of confidential identification (i.e. passwords, biometrics) which is in place and is aligned with industry standards. Supplier shall continuously review, document, grant and revoke access rights for all functional accounts as required and remove or change default passwords and accounts if directly servicing Vodafone.

e) maintain and use strong encryption and security configuration to secure all communication involving Vodafone Information over the network across the relevant network elements whilst in transit or stored, in accordance with industry best practice.

f) protect all Records from loss, destruction, falsification, unauthorised access, and unauthorised release.

g) deliver to all Supplier personnel and, where relevant, contractors and subcontractors, awareness training for security policies and procedures, as relevant for their job function.

h) review their internal security processes and policies, at planned intervals or when significant changes occur, to verify security policies and practices are in line with industry best practice.

i) fully support Vodafone in the meeting of any regulatory or ISO compliance obligation or requirement that may be applicable to the contracted services.

j) provide Vodafone with any requested reports and/or evidence resulting from a penetration test of Information Systems prior to go live.

3.2 Right to Audit

Vodafone reserves the right to conduct audits of the Supplier's adherence to the security requirements outlined in this **Schedule / Agreement**, and the Supplier shall provide full support for these audits whether they are conducted through security assessments or on-site reviews.

4. Security Operational Management

4.1 Incident Management

Supplier shall

a) Manage any information security event or Security Incident in a quick, effective and orderly response.

b) Be responsible for the logging and timely communication of all Security Incidents and all corrective actions and notifications to Vodafone.

c) Review all Security Incidents on a regular basis and update them in accordance with industry best practice until suitably resolved.

d) where appropriate, work with Vodafone's security representatives until the Security Incident or Security Breach has been resolved.

e) register and maintain a list with all administrative access of supplier personnel, contractors and subcontractors that have access to Vodafone premises/Systems and/or Information. Relevant details (excluding personal data) shall be shared with Vodafone, if reasonably requested by Vodafone, for audit, compliance purposes or in case of an incident.

f) notify Vodafone within 48 hours after becoming aware of the Security Breaches /incidents that affect Vodafone in any way (including any potential impact on Vodafone's brand or reputation, or the provision of the contractual services).

- For cyber-Security Incidents and Breaches, report via email csoc@vodafone.com;
- For all other Security Incidents and Breaches (including Personnel and Physical Security, Business Continuity, Fraud, Human Rights), report via email to gcssuppliersincidents@vodafone.com;
- For incidents covering both sections, report to both teams mentioned above.

g) provide a written post report including the root cause of any Security Incident or Breach within 30 days from date of notification of the time of the Incident.

h) Review Security Incidents at least once a year and apply insights gained to introduce mitigation solutions to reduce likelihood of future security incidents.

i) provide an interim fix in the shortest possible time to mitigate the impact of the Security Incident and further resolve the Security Incident within the timelines agreed within the remediation timetable. Where Supplier does not resolve the Security Incident, within the agreed timelines, this shall be deemed a material breach on part of the Supplier.

j) advise any competent public or regulatory authority or law enforcement agency as required and provide all reasonable assistance, including an up-to-date escalation matrix and access to material and/or information to support with such investigations.

4.2 Supplier & External Fourth Party Security

Supplier must manage all security risks related to Fourth Parties. This includes implementing security measures and adding security requirements to Fourth Party agreements (e.g., Incident Response for Security Incidents or Breaches). Supplier shall regularly check Fourth Parties' security compliance and update their service agreements as needed

4.3 Supplier Management

Supplier Shall,

a) participate in Vodafone's supplier assessment process, completing and returning the security risk assessments within 30 days of receiving.

b) participate in, not more than once per year or in case of an incident, in Vodafone's managed business continuity exercises upon mutual agreement.

c) If requested by Vodafone, attend a service and performance review and provide any reasonably requested information prior to the meeting.

d) actively work with Vodafone in support of improving security controls, including but not limited to any future ability for active control monitoring.

4.4 Termination and change of contract

When the Services covered by this Schedule are due to cease as a result of a contract expiring or termination of the Services, Supplier shall;

a) verify that all items of Supplier equipment that contain or hold Vodafone Information or licensed software have had this removed or securely overwritten prior to disposal and provide evidence that these actions are completed as required.

b) notify Vodafone if a change of Service occurs (including where a new or different type of data is processed, stored, or accessed) or where there is a change in the way the service is provided or changes in the Suppliers internal security controls. The Supplier shall support a reassessment to determine any change in security risk.

c) acknowledge that Vodafone reserves the right to vary the terms and conditions if in their opinion there is a change in security risk.

5. Security Core Controls

5.1 Organisational Measures - Corporate Security

5.1.1 Personnel and Physical Security

Supplier shall

a) ensure that security roles and responsibilities of all Supplier employees are clearly defined and documented. Similar requirements shall be imposed by Supplier to its sub-contractors and third parties' contracts.

b) define what breaches of security represent misconduct and the consequences that shall be incurred.

c) carry out background verification checks on all Supplier personnel and contractors who have access to Vodafone Information and Systems, in accordance with relevant laws and regulations. The checks shall be proportional to risks correlated to job roles within the Supplier's organization, with a more rigorous vetting process applied to higher risk roles or roles involving sensitive data or critical asset access. Similar requirements shall be imposed by Supplier to sub-contractors and third parties' contracts.

d) ensure that the employee's background verification checks' status and results are logged and retained and supply written confirmation that these tests have been carried out to Vodafone upon request for audit and compliance purposes.

e) have clearly defined and documented physical security policy and procedures in place. The policy and procedures must be reviewed and updated by the supplier on a regular basis and at least once per year.

f) design and implement physical security controls to protect premises, telecommunications, technology infrastructure, equipment and assets and information facilities from internal, external, and malicious threats or accidents. These controls shall be assessed on a regular basis and at least once per year.

g) have a restrictive access and protect against unauthorized entrance to its premises including information processing facilities from where the Products and Services are provided. Only authorised personnel and approved visitors shall have access. All visitors must be logged, always sign a visitor register and they must be always escorted by appropriate suppliers' personnel. Appropriate physical security controls (i.e., CCTV, security guards, intrusion detection) must be in place to monitor the entry points (i.e., entrance, loading and shipping docks, public access areas) and local area surrounding its facilities.

h) ensure that areas containing sensitive information or critical assets must be physically segregated from general access areas.

i) ensure that surveillance recordings and physical access logs are retained for a minimum of 90 days unless local laws and/or regulations dictates otherwise. Changes to the 90 days need to be communicated in advance.

j) ensure that access rights to supplier premises, telecommunication and information processing facilities are reviewed on a periodic basis.

k) ensure that Media, equipment, information, or software are not removed from the designated premises without prior approval of the appropriate security manager.

l) have a clear desk policy in areas where Vodafone Information is managed or stored. Any documents containing Vodafone Information must be securely stored whether in use or not.

m) where appropriate, ensure that paper documents containing Vodafone Information are transferred in a sealed container / envelope that clearly indicates that the document must be delivered securely to an Authorised User.

5.1.2 Business Continuity Management

Supplier shall

a) ensure that responsibilities for business continuity are clearly defined and documented and have been allocated to an individual with sufficient authority.

b) have a business continuity management programme in place that is aligned with international industry standards (e.g., the international Business Continuity Standard ISO22301). Similar requirements shall be imposed by Supplier to its sub-contractors and third parties' contracts.

c) perform a risk assessment to proactively identify any risks that could cause an interruption to the provision of Products and Services to Vodafone.

d) have business continuity and disaster recovery plan in place to ensure the provision of Products and Services to Vodafone in case of an interruption or failure of business processes in accordance with contractually agreed time frames.

e) have a crisis/incident management plan in place that describes the actions to be taken in case of a Security Incident or event that affects the provision of Products and Services to Vodafone.

f) ensure that the scope of the business continuity and disaster recovery plans and a crisis/incident management plan encompasses all locations, personnel and systems used to provide the contractual services to Vodafone.

g) ensure that the business continuity and disaster recovery plans and a crisis/incident management plan are tested on a periodic basis and at least once per year and shall supply evidence or written confirmation demonstrating that the tests have been performed (including the date and whether the test was successful) to Vodafone upon request for audit and compliance purposes. If the test was unsuccessful, Vodafone has the right to review test results and request improvements if necessary.

h) review and update the business continuity and disaster recovery plans and a crisis/incident management plan on a periodic basis and at least once per year.

i) participate in audits, as per Vodafone's request, in accordance to Right to Audit clause agreed in this document.

j) If the supplier assessment, audit, or review identifies gaps, the supplier must submit a corrective action plan within 30 days outlining the required remediation steps with a reasonable timeline for closure.

5.1.3 Fraud & Investigations

Supplier shall

a) demonstrate their senior management's commitment to conduct business without Fraud.

b) implement and maintain a fraud management process by:

   a. conducting a Fraud Risk Assessment or a Risk Assessment that includes Fraud related questions to proactively identify, document and address vulnerabilities to fraud risks on an ongoing, regular basis.

   b. monitoring and periodically review effectiveness of Fraud management processes.

c) timely, lawfully, and effectively investigate Fraud and other misconduct suspicions or allegations and address any control deficiencies or other issues identified as the outcome of the investigations.

5.2 Technical Measures - Cyber Security

5.2.1 Information Asset classification, handling and protection

Supplier shall

a) Define and use a policy for acceptable use, classify information according to legal and Vodafone contractual requirements, and protect Vodafone information and equipment against unauthorized access, misuse, or manipulation.

5.2.2 Security Hygiene

Supplier shall

a) put in place endpoint protection, antivirus and antimalware, patching and system hardening, and carry out updates on a regular basis in accordance with industry best practice.

b) perform security assessments on information Systems on a regular basis

c) prior to go live of Information Systems, perform a penetration test to detect issues or vulnerabilities, remediate any found issues or vulnerabilities and re-test to confirm the remediation is effective and vulnerabilities are closed. Supplier is liable for all costs resulting from the penetration test.

d) prioritise and remediate all security issues discovered in Products, Services and Systems as set out in the CVSS score matrix contained in Appendix 1.

e) where the Supplier receives their patches and security notes from a 4th party, CVSS score applies - CVSS Score Matrix. shall also apply to the 4th party.

f) provide to Vodafone any relevant security notes and regular patches within the prioritisation and timescales agreed. Documentation shall include severity ratings to allow Vodafone to determine the deployment priority and urgency. Vodafone and Supplier shall each independently test and implement these as required in a timely manner. Apply patches to all Supplier components within defined timescales and industry standards.

g) supply up-to-date guidance on how the Products and Services, including equipment, should be securely deployed.

h) Create and maintain secure, immutable, backup copies of information, software, and system images and test these regularly in accordance with the state of the art and industry best practice,

i) document, review and regularly update a register of external IP address ranges and internet facing systems which allow direct access to the systems from the Internet.

j) maintain rules governing the installation of software by suppliers' users.

k) maintain the secure design, configuration, hardening and management of information Systems, networks, and services to protect against loss of confidentiality, integrity, and availability of Vodafone Information at rest and in transit.

l) enforce Security policies for desktop/laptop clients, networks, applications, databases and operating systems, including but not limited to specific operating system baseline security configurations.

m) maintain a procedure that guarantees password confidentiality and integrity and shall store passwords in a way that makes them unintelligible while they remain valid.

5.2.3 Identity & Access Management

Supplier shall

a) manage and maintain a formal process for granting, modifying, and revoking user access rights. All access rights and identities of all staff, contractors and external party users shall be reviewed at an appropriate security level.

b) use multi-Factor authentication and VPN across all endpoints and in all locations, when accessing any systems, services or networks and restrict access to organisations networks and authorised users.

c) Privileged access shall be via accounts with unique user ID and authentication credentials for each user. Log all activities performed by users with privileged access, and logs are reviewed for malicious activities.

5.2.4 Software Development

Supplier shall

a) develop all Products and Services in a "secure by default" manner.

b) keep separate all development, testing, and operational environments to reduce the risks of unauthorised access or changes to the operational environment.

c) Include the information security related requirements for new information Systems or enhancements to existing information Systems.

d) control changes to systems within the development lifecycle by formal change control procedures.

e) review and test business critical applications when operating platforms are changed to verify there is no adverse impact on organisational operations or security.

f) establish acceptance testing programs and related criteria for new Information Systems, upgrades, and new versions.

g) use test data is selected carefully, protected, and controlled. Supplier shall not use real or 'live' data for testing purposes. If such use is necessary and there is no reasonable alternative, Supplier shall obtain Vodafone's permission prior to testing.

5.2.5 Network Security

Supplier shall

a) maintain security operating procedures including but not limited to the management of intrusion detection and prevention, web application firewall protection, denial of service attack and prevention, and web filtering data loss prevention. Synchronise all clocks of relevant information processing systems to a single reference time source.

b) monitor the network perimeter, all web traffic from the Internet and from internal sources to detect cyber-attacks against web sites / services and block malicious traffic

c) control all changes to firewall rule bases through a formal request / approval process.

d) maintain a network security zoning model which segregates groups of information services, users and information systems and enforces the principle of least privilege.

e) Implement a policy and security measures to manage mobile device security and to protect information accessed, processed, or stored by Authorised Users when working remotely at non office sites.

f) document all access to Vodafone systems to support and monitor that the respective services are reviewed and approved by Vodafone if required.

5.2.6 Security Logging & Monitoring

Supplier shall

a) maintain security operating procedures including but not limited to the management of security event logging and monitoring and shall review them on a regular basis and update them as required in accordance with state of the art or industry best practice.

b) Produce and keep event logs recording user activities, exceptions, faults, and information security events and shall review these for malicious activities.

c) Protect all logging facilities and log information against tampering and unauthorised access and shall store/delete log files in line with the agreed retention periods.

Annex 1 - Vulnerability and issue fixing timelines

Issue rating	Issue Definition (Level of risk must take into account existing countermeasures)	Timeline
EMERGENCY	Critical Vulnerability (typically CVSS score 10) that can be actively exploited from an untrusted network without any need to authenticate on the asset.	Must not exceed 7 calendar days under any circumstances.
CRITICAL	Critical rated vulnerability (typically CVSS score 9-10) is identified.	Must never exceed 30 calendar days under any circumstances.
HIGH	High rated vulnerability (typically CVSS score 7.0-8.9) is identified.	Within 30 calendar days for internet facing assets OR 90 days or internal assets
MEDIUM or LOW	Medium or Low priority vulnerability (typically CVSS score 0.1-6.9) is identified.	Within 90 calendar days