INFORMATION SECURITY ANNEX VODAFONEZIGGO

January 2023

Contents

1 PURPOSE

This Annex sets out the minimum security requirements the Supplier shall adopt relevant to the relevant scope of work being undertaken, aiming to protect VodafoneZiggo and its customers. Parties are responsible to ensure ongoing compliance with these requirements where applicable to that party and to identify and act on acts or areas of non-compliance. The parties recognize that information security techniques, and the existing threats to security are continually evolving. Therefore, Supplier shall undertake holistic and comprehensive assessments of security depending upon the circumstances and the type of data and processing to be performed in order to determine and apply an appropriate level of protection.

The Supplier shall apply these requirements as specified in this Annex. To the extent applicable, the requirements in this Annex shall be complementary to and not conflicting with any other general security requirements as applicable and agreed to by the parties (such as any further security requirements as are identified in any pre- or post-contract security assessment(s)).

These requirements are not intended to be specific to the processing operations undertaken by Supplier on behalf of VodafoneZiggo. Rather, Supplier shall adopt these standards as appropriate standards designed to ensure a secure operating environment generally.

2 DEFINITIONS

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

Term	Definition
4th Party	means the Supplier's contractors and their subcontractors (of any tier) who perform activities through the Supplier related to the Products and Services defined in the Agreement (and have no contractual relations with VodafoneZiggo directly).
Administrative User	Refers to an Authorized User who has access to administrative user account(s): accounts used in the performance of the Services under the Agreement by administrators to perform administrative tasks (users with named admin accounts) such as on servers, databases or network switches.
Authorised Users	means employees, officers, directors or contractors of Supplier who have a legitimate operational need and are authorized to access Information Systems or carry out any processing of VodafoneZiggo Information.
Data Record	means any information (in whatever form) created, received and maintained as evidence and as an asset by the company or

	employee, in pursuit of legal obligations or in the transaction of business.
Information Systems	means all systems enabling communication and used to access, create, modify, store, transmit or otherwise process or use VodafoneZiggo Information, including temporary files.
Internet facing	means systems or applications that are reachable from the internet without needing to connect to an internal network via a VPN. Cloud assets which are accessible from the internet are to be considered internet facing.
Media	means a physical object likely to be processed in an Information System and on which data may be recorded or from which they may be retrieved.
MFA (Multi Factor Authentication)	means a user access authentication method that requires the user to provide two or more verification factors to gain access to a resource (such as an application, online account, or a VPN). Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors.
Products and Services	means the products and services provided by the Supplier under the Agreement.
Patching	Means a set of changes to an application and/or server, storage and network (infrastructure) or its supporting data, designed to update, fix or improve it. This includes fixing security vulnerabilities and other bugs. Patches are often written to improve the functionality, usability, or performance of a program.
SSDLC (Secure Software Development Life-Cycle)	Means Secure Software Development Lifecycle. The SSDLC standard integrates security into the software development process, resulting in the security requirements being gathered alongside functional requirements, risk analysis being undertaken during the design phase, and security testing happening in parallel with development, for example.
Security Breach	means the accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, VodafoneZiggo Information or Information Systems. For the avoidance of doubt, if

	any fraudulent act leads to the unauthorized access, disclosure or use of VodafoneZiggo Information or VodafoneZiggo Systems, such act will be considered a Security Breach.
Security Incident	means any event which causes, or could lead to, a disruption in the provision of the contractual service(s) and/or an actual impact to the confidentiality, integrity or availability of VodafoneZiggo Information and Information Systems.
Security 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.
Supplier Personnel	All persons engaged by or on behalf the Supplier used in the performance of its obligations under the Agreement, including the Supplier's employees, agents, consultants, contractors as well as Supplier's subcontractors and third parties (and their personnel).
User Identity	means the personal and unique identification code issued to every Authorised User.
VodafoneZiggo Information	means information, in whatever form, such as text, audio, video, image files and other form(s) of data, to be provided by, processed by and/or accessed to by the Supplier in connection with the provision of the Products and Services under the Agreement..
Personal Data	shall mean any information relating to an identified or identifiable natural persons or as otherwise defined in applicable Privacy Laws.
Privacy Laws	means all applicable laws and regulations relating to the processing of Personal Data and privacy that may exist in the relevant jurisdictions (including but not limited to the EU General Data Protection Regulation (GDPR).
Privileged Access	means a designates special access or abilities above and beyond that of a standard Authorized User. Also known as system administrator accounts, privileged access accounts give users elevated, frequently unrestricted access to a company's underlying information systems and infrastructure.

Products and Services	means the products and services provided by the Supplier under the Agreement
VOG	refers to the Certificate of Conduct ("*Verklaring Omtrent het Gedrag (VOG*") document that can be requested at the Integrity and Screening Agency (Justis) of the Dutch Ministry of Justice and Defence in the Netherlands. The VOG provides a certificate showing that past (judicial) conduct of a person forms no obstacle to performing a specific task or job at an employer or in the society.

3 GENERAL

3.1 COMPLIANCE

Supplier shall in alignment and approval with VodafoneZiggo:

a) have a process in place to
   a. identify, document, and keep up to date all requirements in this Annex and any additional security appendices;
   b. review the security requirements as stated in this Annex and any additional security appendices to ensure achievement and maintenance of compliance;
   c. provide a complete and accurate report on VodafoneZiggo's request, detailing points of non-compliance to the requirements in this Annex and any additional security appendices;

b) ensure that security measures taken in the technical and physical work environment that is used to provide the Products and Services to VodafoneZiggo are comparable to those of the of the Supplier's at the time of concluding the Agreement;

c) ensure that responsibilities for compliance with these minimum security requirements are clearly defined and documented and have been allocated to individuals with sufficient authority (e.g.: a CISO or Security Officer), who can be reached by means of the communication or escalation model. The individuals shall be trained and experienced in managing security, and shall be provided with appropriate resources to effectively ensure compliance. Supplier shall provide the contact details of the individual to VodafoneZiggo upon entering into the Agreement or, alternatively, agree on the communication or escalation model

through which the individual can be contacted and shall promptly notify VodafoneZiggo of any changes to such details;

d) Upon VodafoneZiggo's request, Supplier shall aim within 10 working days to provide initial evidence of the status of its security controls (e.g., ISO27001, ISO22301, SOC2, security risk rating service report etc.) that is acceptable by VodafoneZiggo and any security requirements set by law or regulation. If such evidence is not provided, the Parties shall agree a reasonable date to obtain such evidence and Supplier shall provide it accordingly to VodafoneZiggo;
e) define, allocate and formally document security responsibilities. This information shall be reviewed on a regular basis and updated by Supplier as required to reflect organisational and personnel changes where these impacts the terms of the Agreement;
f) formally document and publish the Supplier's security standards, and share a compliance status at the request of VodafoneZiggo to demonstrate Supplier's adherence to the security standards;
g) protect all Data Records from loss, destruction, falsification, unauthorised access, and unauthorised release;
h) review the approach to managing security and its implementation (i.e. control objectives, controls, policies, processes and procedures for security) independently at planned intervals or when significant changes occur.

3.2 SECURITY INCIDENT RESPONSE

Supplier shall:

a) have a formal and documented incident management process in place including the handling of Security Incidents, with defined roles and responsibilities;
b) log all Security Incidents. Supplier shall make these available to all Authorised Users who need them, and shall review them on a regular basis and update them as required in accordance with industry best practice;
c) define, document, implement and maintain a procedure for reporting, responding to and managing Security Incidents and Security Breaches in line with the targeted timelines set in Appendix 1. This shall include as a minimum:
    i. a procedure for reporting such Security incidents and Security Breaches to appropriate stakeholders ;
    ii. a clearly designated team for managing and co-ordinating the response to a Security Incident
    iii. a documented and tested process for managing the response to a Security Incident, including the requirement to keep appropriate issues and action logs to include the time at which the Security Incident occurred, the person reporting the Security Incident, to whom it was reported and the effects thereof;

iv. the requirement on the Supplier to notify VodafoneZiggo immediately if it appears if VodafoneZiggo Information was involved in the Security incident or Security Breach and was impacted or affected in some way; and

v. the Supplier shall promptly provide a motivated response to all additional requests from VodafoneZiggo related to the Security Incident or Security Breach and work together and cooperate with VodafoneZiggo's security representatives until the Security incident or Security Breach has been satisfactorily resolved.

d) test the procedure for reporting, managing, and responding to Security Incidents at defined regular intervals and at least once (1x) per calendar year, and shall provide to VodafoneZiggo all findings from the tests of the procedure for reporting, managing, and responding to Security Incidents in line with timelines set in Appendix 1.

e) report and notify VodafoneZiggo in writing of any Security Incident or Security Breach, that affect VodafoneZiggo in any way (including any potential impact on VodafoneZiggo's brand or reputation, or the provision of the contractual services) as specified in Appendix 1. The notification should be reported to VodafoneZiggo by sending an email to the CSIRT team at CSIRT@vodafoneziggo.com.;

f) In the event of a Security Breach or a Security Incident, the Supplier shall be responsible for the corrective actions and notifications to VodafoneZiggo and include in the notification to VodafoneZiggo

i. a detailed description of the Security Incident or Security Breach,

ii. in case known by the Supplier, the classification of data that was the subject of the Security Incident or Security Breach and;

iii. the identity of each affected person (or, where not possible, the approximate number of data subjects and of Personal Data Records concerned) if the Security Incident or Security Breach affects Personal Data and

iv. the name and contact details of an appropriate Supplier point of contact where more information can be obtained and

v. a description of the likely consequences of the Security Incident or Security Breach and

vi. a description of the measures taken or proposed to be taken by Supplier to address the Security Incident or Security Breach, including, where appropriate, measures to mitigate its possible adverse effects; and additionally in such notification or thereafter and

vii. as soon as such information can be collected or otherwise becomes available, any other information VodafoneZiggo may reasonably request relating to the Security Incident or Security Breach.

g) provide a written Post Security Incident Report including the root cause of Security Incidents or Security Breaches according to timelines set per priority in Appendix 1 and, if applicable, a remediation plan including targeted mitigation timelines and action owners.;
VodafoneZiggo shall have the right to request changes to the remediation plan or timetables. Both Parties shall agree and sign off on the agreed remediation

plan. Supplier shall be required to provide an interim fix in the shortest possible time and further resolve the weaknesses within the timelines agreed within remediation timetable where Supplier does not resolve weaknesses, within the agreed timelines, this shall be escalated as per the agreed escalation model All progress and mitigation actions taken shall be communicated by the Supplier in writing to VodafoneZiggo;

h) cooperate fully with VodafoneZiggo during any investigation by VodafoneZiggo and/or any competent public or regulatory authority or law enforcement agency, providing reasonable assistance and access to material and/or information to support with such investigations.

3.3 SUPPLIER & EXTERNAL 4TH PARTY SECURITY

Supplier shall:

a) obtain permission to outsource or share VodafoneZiggo Information beyond the Supplier's own organisation, solely in order to (be able to) provide the Products and Services as agreed within the Agreement. VodafoneZiggo should be made aware and asked to agree granting activities to 4th Parties, that is any subcontractor or other company who have only commercial links with the Supplier and not with VodafoneZiggo; define, document, implement and maintain security principles and requirements for mitigating the risks associated with 4th Parties and their access to processing or hosting assets or provision of VodafoneZiggo network & IT infrastructure;
b) include information security requirements in its agreements with 4th Parties that equal the ones set out between VodafoneZiggo and the Supplier;
c) include an obligation of prompt notification of Security Breach(es) in its agreements with 4th Parties;
d) monitor and review the achievement and maintenance compliance of 4th Parties security against these requirements and service delivery on a regular basis;
e) manage the changes to the provision of products and services by the 4th Parties, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

3.4 TERMINATION / CHANGE OF CONTRACT SCOPE

Supplier shall:

a) When the provision of Products and Services covered by the Agreement are due to cease as a result of a termination or expiration of the Agreement:
    i. ensure that all items of equipment containing storage are verified to confirm that any VodafoneZiggo Information and licensed software has

been removed or securely overwritten prior to disposal (e.g., at the end of contract, following a hardware failure) or re-use;

ii. provide evidence that each of these actions was completed as required within 30 days after termination or expiration of the Agreement

b) notify VodafoneZiggo if a change of Product or Service occurs where a new or different type of data is processed, stored, or accessed;

c) engage upon request of VodafoneZiggo to renegotiate terms and conditions during the Agreement or at defined regular intervals due to changes of information security risk;

d) together with VodafoneZiggo define an exit plan and the terms on which VodafoneZiggo has a right to exit or terminate the Agreement including circumstances of non-compliance to the requirements andconditions set out in this Annex. VodafoneZiggo is entitled and has a right, upon need and at its sole discretion, to engage in commercial conversations with the Supplier on terminating the Agreement in case the Security Breach is handled with insufficient compliance to the security incident response measures set out in this Annex.

3.5 RIGHT TO AUDIT

Supplier shall permit VodafoneZiggo, its respective sub-contractors, auditors, or other agents (each an "Auditing Party"), to access Supplier's premises, computer and other Information Systems, records, documents, and agreements as reasonably required by the Auditing Party to check that Supplier is complying with the requirements under this Annex. Any review in accordance with this paragraph shall not require the review of any third-party data and the Auditing Party may be required to enter into a confidentiality agreement with Supplier as may be reasonably necessary to respect the confidentiality of the information of which the Auditing Party may become aware in the course of undertaking the review. Each Party shall bear its own costs in relation to such audit, unless the audit reveals any non-compliance with Supplier's obligations under this Annex, in which case the costs of the audit shall be borne by the Supplier.

4 ORGANISATIONAL MEASURES

4.1 PERSONNEL SECURITY

Supplier shall:

a) ensure that security roles and responsibilities of all Supplier personnel (employees, contractors and sub-contractors) are clearly defined and documented;

b) register and maintain a list with all Supplier personnel (employees, contractors and subcontractors) with Administrative User access granted to VodafoneZiggo Information, Information Systems and assets. This list and its' updates shall be shared with VodafoneZiggo;
c) have a comprehensive disciplinary process in place, which clearly defines the procedures that follow upon failure to comply with Supplier's security policies, standards, or requirements, such as investigation which may result in disciplinary action up to and including termination of employment or engagement by Supplier, if Supplier sees necessary;
d) carry out background verification checks on all Supplier personnel (employees, contractors and subcontractors) who have access to VodafoneZiggo Information and Information Systems, in accordance with relevant laws and regulations. The checks shall be proportional to risks correlated to job/function roles within the Supplier's organization, at Suppliers' discretion.
e) in accordance with the Dutch Regulation on safety and integrity telecommunication ("*Regeling veiligheid en integriteit telecommunicatie (RVIT)*"), for all Supplier personnel (employees, contractors and sub-contractors) performing (particular) network management tasks (as stated in RVIT), a VOG screening (referenced in Appendix 3) or equivalent screening framework outside of the Netherlands, is required to be performed prior to performance of such tasks by Supplier personnel. (Copies of) the results of these VOG screening are required to be shared with VodafoneZiggo before performance of such tasks by Supplier personnel;
f) upon request of VodafoneZiggo, inform and, to the extent necessary, provide written proof to VodafoneZiggo of its employees' and contractors' responsibilities for security as included in their contractual (employment) agreements;
g) where appropriate, update checks as mentioned in above articles (a-f) are performed on defined regular intervals, at least once (1x) per calendar year
h) when requested by VodafoneZiggo, Supplier will confirm that background verification checks and VOG screenings and results are logged and retained in accordance with Supplier's own retention policy, however, VodafoneZiggo will not require access to the actual background checks, VOG screenings and results, nor to Supplier's retention policy; ensure that the background verification checks' status and results are logged and retained and supply evidence that these tests have been carried out to VodafoneZiggo upon request for audit and compliance purposes; when requested in writing, Supplier will confirm in writing that its employees' and contractors' responsibilities for security are included in their contractual (employment) agreements, however, VodafoneZiggo will not require access to the actual contractual (employment) agreements.;
i) ensure that all Supplier personnel and, where relevant, contractors and subcontractors receive appropriate awareness and training for security policies and procedures, ensuring the Supplier's employees and contractors are trained on the Supplier's security policies and made aware of the responsibilities to

security practices . The trainings are to be provided at least at startup and refresher trainings according to Supplier's personnel security policies;

4.2 PHYSICAL SECURITY

Supplier shall:

a) ensure that responsibilities for physical security are clearly defined and documented and have been allocated to an individual with sufficient authority (e.g.: a CISO or Security Officer);
b) have a clearly defined and documented physical security policy and procedures in place. The policy and procedures must be reviewed and updated on a regular periodic basis and at least once (1x) per calendar year.
c) design and implement physical security controls to address internal and external risks to its premises and information processing facilities. These controls shall be assessed on a regular periodic basis and at least once (1x) per calendar year;
d) define and use security perimeters to protect its information processing facilities and locations storing VodafoneZiggo Information;
e) inspect the local area surrounding and its facilities used for the provision of Products and Services for risks and threats on a regular periodic basis and at least once (1x) per calendar year;
f) have secure entry points in its premises and information processing facilities from where the Products and Services are provided, that restrict access and protect against unauthorised access. Only authorised personnel and approved visitors shall have access. All visitors must be logged, sign a visitor register and escorted by appropriate suppliers' personnel at all times. 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);
g) ensure that logs detailing physical access are kept for at least 90 (ninety) days;
h) ensure that Supplier personnel and approved visitors are issued access identification cards at premises that allow access to VodafoneZiggo Information and/or Information Systems. Visitors' cards must be clearly distinguished from supplier personnel's access identification cards.
i) have a comprehensive process in place to ensure that access rights to Supplier premises and information processing facilities are reviewed on a regular basis;
j) design and apply reasonable physical protection measures against malicious attack or accidents; where possible, ensure that media, equipment, information or software are not removed from the designated premises without prior approval of the appropriate role;
k) apply security to off-site assets taking into account the different risks of working outside its premises and information processing facilities;

l) have a clear desk policy in areas where VodafoneZiggo Information is managed or stored. Any documents containing VodafoneZiggo Information must be securely stored when they are not in use;
m) have a clear screen policy for its information processing facilities;
n) where appropriate, ensure that paper documents containing VodafoneZiggo Information are transferred in a sealed container / envelope that clearly indicates that the document must be delivered by hand to an Authorised User.

4.3 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 (e.g.: a CISO or Security Officer);
b) have (and ensure that its subcontractors have) a business continuity management programme in place that is aligned with industry best practices or standards (e.g., the international Business Continuity Standard ISO22301);
c) perform a risk assessment to proactively identify any risks that could cause an interruption to the provision of Products and Services to VodafoneZiggo;
d) have business continuity and disaster recovery plans in place to ensure the provision of Products and Services to VodafoneZiggo in case of an interruption or failure of business processes in accordance with contractually agreed time frames;
e) ensure that the scope of the business continuity plan encompasses all locations, personnel and information processing systems used to provide the Products and Services to VodafoneZiggo;
f) ensure that the business continuity and disaster recovery plans are tested on a regular periodic basis, being at least once (1x) per calendar year or at a frequency that has been agreed with VodafoneZiggo and shall supply evidence demonstrating that the tests have been performed (including the date and whether the test was successful) to VodafoneZiggo upon request for audit and compliance purposes;
g) review and update the business continuity and disaster recovery plans on a regular periodic basis and at least once (1x) per calendar year;
h) notify VodafoneZiggo in the event of an interruption which impacts the provision of Products and Services to VodafoneZiggo;
i) have a crisis management plan in place that describes the actions to be taken in case of an incident or event to ensure the provision of Products and Services to VodafoneZiggo.
j) upon mutual agreement participate and cooperate in VodafoneZiggo's managed business continuity exercises or audits as requested by VodafoneZiggo.

4.4 DATA MANAGEMENT

Supplier shall:

a) treat VodafoneZiggo Information according to their information classification category (see chapter Information Asset Classification & Handling), and safeguard it accordingly ensuring that it is not released publicly;
b) not store, copy, disclose or use VodafoneZiggo Information except as necessary for the performance by the Supplier of its obligations under the Agreement, or as otherwise expressly agreed or authorised in writing by VodafoneZiggo;
c) ensure that the creation of VodafoneZiggo Information is limited to the minimum necessary in the support of VodafoneZiggo, or to comply with legal obligations.
d) limit the access of VodafoneZiggo Information to authenticated Authorised Users and monitor the flow of data to subcontractors;
e) if the Supplier subcontracts any processing of VodafoneZiggo Personal Data, they shall notify VodafoneZiggo in advance of such processing and obtain VodafoneZiggo's prior written permission before processing;
f) ensure proper handling and disposal of VodafoneZiggo Information from Supplier Information S ystems:
    i. safe disposal of data records must be conducted to ensure that relevant security measures are applied and that any restrictions on manner of destruction, for example security and confidentiality, are not breached;
    ii. inventory all VodafoneZiggo Information prior to disposal and certify in writing to VodafoneZiggo that it has been securely deleted or destroyed;
    iii. physical Data Records must be destroyed in an environmentally friendly manner.

5 TECHNICAL MEASURES

5.1 INFORMATION ASSET CLASSIFICATION & HANDLING

Supplier shall:

a) define, document, implement and maintain rules for the acceptable use of information and of assets associated with information and information processing facilities, and shall communicate these to all users;
b) define, document, implement and maintain a policy addressing the classification of information in terms of legal requirements, value, criticality and/or sensitivity to unauthorised disclosure or modification, and shall review such policy on a regular periodic basis, at least once (1x) per calendar year, and update it as required. The methodology used by Supplier to classify the information must consider the risks involved with the loss of confidentiality, integrity and availability of the information;

c) define, document, implement and maintain procedures for information labelling in accordance with the information classification scheme adopted and shall communicate such labelling procedures to users, and, where feasible, shall technically enforce those procedures;
d) where possible, define, document, implement and maintain information classification and labelling covering media, services and systems provided to VodafoneZiggo in accordance with the information classification scheme chosen by Supplier;
e) ensure that media containing VodafoneZiggo Information, and printed copies of this data, are clearly and minimally marked as confidential.

5.2 INFORMATION PROTECTION

Supplier shall:

a) implement appropriate measures designed to protect media containing VodafoneZiggo Information against unauthorised access, misuse or corruption at rest and during transportation;
b) define, document, implement and maintain a policy on the use of cryptographic controls and the protection and lifetime of cryptographic keys in accordance with the state of the art and industry best practice;
c) define, document, implement and maintain mechanisms designed to protect equipment when unattended, e.g. through using device locks and password protected screen locks;
d) implement access controls and strong encryption designed to protect information from unauthorised access and modification in transit and at rest;
e) only distribute VodafoneZiggo Information if the data have been strongly encrypted to guarantee that it is not intelligible or is not manipulated in transit;
f) define, document, implement and maintain a policy and supporting security measures covering privacy and protection of Personal Data to comply with the relevant applicable laws, legislation and regulation, including ensuring that:
    i. where anonymisation is applied, data must be rendered anonymous in such a way that the data subject is permanently no longer identifiable;
    ii. where pseudonymisation techniques are used, technical (e.g., strong encryption, hashing or tokenisation) and organisational (e.g., agreements, policies, privacy by design) measures separating pseudonymous data from an identification key must be in place to mitigate the risk of unauthorised reversal of pseudonymisation;
g) define, document, implement and maintain a formal process designed to identify and assess critical assets associated with information and information processing facilities in a consistent way considering confidentiality, data privacy, resilience, compliance and other aspects as applicable. Supplier shall maintain a register of the critical assets and review it on a regular periodic basis for completeness and accuracy, and update it as required;

h) define, document, implement and maintain technical procedures for recording incoming and outgoing media to control the flow of VodafoneZiggo Information and record:
    i. timing of transmission or transfer,
    ii. the type of VodafoneZiggo Information transmitted or transferred,
    iii. the destination of the VodafoneZiggo Information,
    iv. how the VodafoneZiggo Information is transmitted or transferred,
    v. details of the Authorised User(s) conducting the transmission or transfer,
    vi. and the destination of VodafoneZiggo Information being transmitted or transferred;
i) ensure that the minimum details to be recorded for every access to the VodafoneZiggo Information include information giving the ability to identify who accessed the VodafoneZiggo Information and when. The minimum period for retaining the VodafoneZiggo Information recorded shall be specified by Supplier in accordance with the state of the art and industry best practice, and where applicable with the agreed data retention period
j) monitor transactions, transmissions or transfers resulting VodafoneZiggo Information leaving endpoints and where sensitive and VodafoneZiggo Information is identified Supplier shall ensure that a Security Incident process gets triggered and the transaction gets blocked or strong encryption of the VodafoneZiggo Information is enforced as required;
k) define, document, implement and maintain procedures for the management of removable media in accordance with Supplier's classification scheme;
l) ensure that Media is disposed of securely when no longer required according to formally defined procedures where the method being used is aligned with the classification of the contained VodafoneZiggo Information.

5.3 SECURITY HYGIENE

Supplier shall:

a) define, document, implement and maintain security operating procedures including the management of endpoint protection, antivirus and antimalware, patching and system hardening, and where available, make such procedures available to all users who need them, review them on a regular periodic basis and at least once (1x) per calendar year, and update them as required in accordance with industry best practice;
b) perform security assessments on live information systems including supplied software on a regular basis, designed to detect deviations or vulnerabilities.
    i. Supplier shall promptly report findings of vulnerabilities to VodafoneZiggo, in line with the timeline defined in Appendix 1.
    ii. Supplier shall also perform a risk assessment on issues and vulnerabilities found, followed by a remediation (e.g., through patching, system upgrades or configuration changes) and a re-test to confirm the remediation is effective and vulnerabilities are closed.
    iii. Supplier shall implement compensating controls and / or risk acceptance process within defined timescales;

c) perform vulnerability assessments and testing prior to go-live of Information Systems and remediate any medium or higher rated vulnerabilities prior to go-live;
d) perform vulnerability assessments and penetration tests on a regular basis in accordance with the state of the art and industry best practice. Supplier shall also complete a risk assessment, followed by remediation of identified issues within defined timescales;
e) define, document, implement and maintain a vulnerability and issue fixing process including prioritisation definitions and required resolution timescales. Supplier shall identify and define any gaps in Information Systems, assign a priority to them and fix all gaps within those resolution timescales. Supplier shall support and maintain the security of Products and Services including all equipment, and all software and hardware subcomponents throughout the term of the Agreement including end of life; such maintenance, as a minimum, shall cover security fixes;
f) prioritise and remediate all security issues discovered in Products, Services and Information Systems as set out in the Agreement (including where the Supplier requires a patch and/or security note from a 4th Party) . Supplier shall provide regular updates on progress in the interim. This requirement shall apply to all Products, Services and Information Systems impacted by the vulnerability, not only the Products, Services and Information Systems for which the vulnerability was notified;
g) where the Supplier receives their patches and security notes from a 4th Party, requirements detailed in Appendix 1 shall also apply to such 4th Party;
h) proactively provide to VodafoneZiggo relevant security notes and regular patches within the prioritisation and timescales set out in Appendix 2, including those relating to feature releases, new product releases or additional functionalities of the Products, Services and Information Systems;
i) provide sufficient documentation, including severity ratings, alongside all security notes and patches to allow VodafoneZiggo to determine the deployment priority and urgency;
j) provide and apply patches to all Supplier components including, but not limited to operating systems, databases, webservers, and applications; within defined timescales and industry standards.
k) when VodafoneZiggo receives security notes and related patches from the Supplier, VodafoneZiggo and Supplier shall each independently test and implement these as required in accordance with the timelines as set in Appendix 2.. The process for testing and implementing security notes and related patches shall be performed on a regular periodic basis and in accordance with industry best practice. Upon request of VodafoneZiggo, Supplier shall be able to demonstrate such process and in accordance with the VodafoneZiggo Vulnerability, patching and issue fixing timelines as set out in Appendix 2;
l) supply up-to-date guidance on how the Products and Services, including equipment, should be securely deployed;
m) protect endpoints, servers, storage devices, mail / web gateways and mail traffic with active anti-malware tools where technically feasible to detect and wherever possible prevent malware infections;

n) define, document, implement and maintain tools to prevent the unintended deterioration or destruction of VodafoneZiggo Information (for example by viruses, malware/ransomware or other harmful programmes);
o) define, document, implement and maintain procedures for making back-up copies and for recovering VodafoneZiggo Information. These procedures shall guarantee that data files can be reconstructed in the state they were in at the time they were lost or destroyed and enable the full restoration of the service within agreed timescales;
p) create secure, immutable, backup copies of information, software, and system images and shall test these regularly in accordance with the state of the art and industry best practice;
q) keep a back-up copy and data recovery procedures at a different location from the site of the information Systems processing the VodafoneZiggo Information, where hosted managed services are being provided, and these security requirements shall apply to such back-up copies;
r) protect logging facilities and log information against tampering and unauthorised access, and shall store/delete log files in line with the agreed retention periods, which are in accordance with the VodafoneZiggo detailed policy on creating and documenting retention rules. The exact retention periods can vary and are set by the respective data owner of VodafoneZiggo, who shall communicate the retention periods to the Supplier ;
s) 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;
t) define, document, implement and maintain rules governing the installation of software by Authorized Users;
u) define, document, implement and maintain standards for the secure design, configuration, hardening and management of information Systems, networks, and services to protect against loss of confidentiality, integrity, and availability of VodafoneZiggo Information at rest and in transit;
v) consistently implement formally documented and approved security standards for desktop and laptop clients for new / newly configured client and security settings to prevent end users from changing them on their client;
w) formally document and publish security standards for networks, applications, databases and operating systems, including but not limited to specific operating system baseline security configurations. Supplier shall review these standards on a regular basis and update them as required;
x) define, document, implement and maintain a procedure that guarantees password confidentiality and integrity and shall store passwords in a way that makes them unintelligible while they remain valid;
y) remove or change default passwords and accounts if directly servicing VodafoneZiggo.

5.4 IDENTITY & ACCESS MANAGEMENT

Supplier shall:

a) define, document, implement and maintain a process covering the formal registration of Authorized Users belonging to Supplier Personnel and any 4th Parties who perform activities as part of the Products and Services as set out in the Agreement and who can access VodafoneZiggo Information, with a unique identity as prerequisite for granting any access to the user, and de-registration of users in order to support the timely revocation of access rights;
b) define, document, implement and maintain a formal process for where the use of functional accounts (used by systems / applications) or shared accounts (used by multiple individuals) are necessary for business or operational reasons to supply Products and Services under the Agreement, and shall maintain the documentation and assignment of a responsible owner;
c) define, document, implement and maintain a formal process for granting, modifying and revoking user access rights;
d) implement appropriate measures designed to ensure that all access rights and identities of all personnel, staff, contractors and external party users shall be reviewed by responsible management upon change of their role, adjusted / removed as required and are locked or removed upon termination of their employment, contract or agreement in a timely manner;
e) revoke user access if it has not been used in line with the timeline set in Supplier's access management policies, whereby the target timeline for being inactive shall be a maximum of six (6) months;
f) review user identities and user access rights on a regular basis, at least at yearly intervals, to confirm that they continue to be still required;
g) control the process of granting and provisioning privileged access and assign it only to a separate account different from that used for regular business activities;
h) Privileged Access shall be via accounts with unique user ID and authentication credentials for each user and these shall not be shared and shall be via accounts secured with Multi Factor Authentication (MFA). Username and password authentication shall be stored in a centralized service with appropriate role-based access control which is updated by the joiners, leavers, and movers process, keep an up-to-date record of Authorised Users, and the authorised access available to each, and shall establish identification and authentication procedures for all access to Information Systems or for carrying out any processing of VodafoneZiggo Information;
i) ensure that activities performed by Authorized Users with Privileged Access are logged, and shall review logs for malicious activities;
j) restrict access to information and application system functions by a secure log-on procedure which meets at minimum the following requirements:
    i. the use of passwords which are compliant with the agreed password policies is enforced by the Supplier;
    ii. passwords shall consist of at least 8 (eight) characters, or, if this is not technically permitted by the relevant Information System, a password shall consist of the maximum permitted number of characters.

iii. passwords shall not contain any item that can be easily related to the Authorised User and must be changed at regular intervals, at least every 90 (ninety) days. Passwords shall be modified by the Authorised User to a secret value known only to them when it is first used as well as at least every 90 (ninety) days thereafter;
iv. passwords are not displayed during entrance/access and are not transmitted in clear text over a network;
v. log-on information is validated only on completion of all input data;
vi. accounts are locked or blocked for a period of time after a number of predefined unsuccessful log-on attempts, at least after 5 (five) failed attempts;
vii. unsuccessful and successful attempts are being logged and security events are raised if a potential attempt or successful Security Incident or Breach of log-on controls is detected;
viii. inactive sessions are terminated or locked after a defined period of inactivity.

5.5 SOFTWARE DEVELOPMENT

Supplier shall:

a) implement appropriate measures designed to ensure software development is executed in line with a best practice Secure Software Development Life-Cycle (SSDLC) standard or guideline. It is ensured that development, test, and production environments are separated to reduce the risks of unauthorised access or changes to production data.
b) ensure that all new and updated software (including generic components such as operating systems) is fully patched at the time of deployment, meets established hardening requirements and is upgraded to versions that are still actively supported.
c) undertake any testing in non-production environments for Products and Services supplied to VodafoneZiggo. Supplier shall not use VodafoneZiggo Information for testing purposes. If such use is necessary and there is no reasonable alternative, Supplier shall obtain VodafoneZiggo's prior written consent for testing with VodafoneZiggo Information, and such use shall be limited to the extent necessary for the purposes of testing and Supplier guarantees the level of security corresponding to the type of VodafoneZiggo Information processed;
d) ensure that information security related requirements are included in the requirements for new Information Systems or enhancements to existing Information Systems;
e) control changes to systems within the development lifecycle by formal change control procedures;

f) review and test business critical applications when operating platforms are changed to ensure there is no adverse impact on organisational operations or security;
g) establish acceptance testing programs and related criteria for new Information System upgrades and new versions;
h) immediately report vulnerabilities in the supplied software and provide updates or patches in accordance with acknowledged resolution times as set out in Appendix 2 1, (depending on the severity of the vulnerability) to fix them.

5.6 SECURITY EVALUATION OF SOFTWARE PRODUCTS

Supplier shall:

a. enable and work with VodafoneZiggo that prior to rollout, an appropriate (technical) security evaluation or penetration test is carried out on software products, either by VodafoneZiggo itself or by a third party independent of the Supplier;
b. demonstrate to VodafoneZiggo that production software deployed in the infrastructure is the same as the software evaluated;
c. provide updates to VodafoneZiggo with follow-up of findings of the identified vulnerabilities (in line with the conditions as set out in the Security Hygiene chapter and in Appendix 1) and the software product will not be put in use until the findings have been resolved.

5.7 NETWORK SECURITY

Where and as applicable, Supplier shall:

a) define, document, implement and 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. Where possible, Supplier shall make these procedures available to all users who need them, and review them on a regular basis and update as required in accordance with industry best practice;
b) define, document, implement and maintain strong encryption and security configuration standards to secure all communication involving VodafoneZiggo Information over the network across the relevant network elements;
c) ensure that the clocks of all relevant information processing systems are synchronised to a single reference time source;
d) monitor the network perimeter to detect cyber-attacks and block malicious traffic;
e) monitor web traffic from the Internet and from internal sources to detect cyber-attacks against web sites / services and block malicious traffic;

f) ensure that changes to firewall rule bases are controlled through a formal request / approval process, and is regularly monitored;
g) restrict access to the organisation's networks to authorised devices and control this using digital certificates;
h) define, document, implement and maintain a security zoning model for the networks which segregates groups of information services, users and Information Systems and enforces the principle of least privilege. Supplier shall control/restrict access between security zones by physical separation of networks or via gateways;
i) define, document, implement and maintain a policy and supporting security measures to manage mobile device security;
j) define, document, implement and maintain a policy and supporting security measures to protect information accessed, processed, or stored by Authorised Users when working remotely at non office sites. Access to the Supplier's network shall be secured by use of a Virtual Private Network (VPA) and MFA (Multi Factor Authentication). Endpoints shall be secured with controls including: no local admin privileges, up to date anti-malware and antivirus, restricted internet browsing, and disk encryption for the storage used.
k) define, document, implement and maintain Multi Factor Authentication (MFA) on endpoints / mobile devices which can be used to access services, systems, and networks from the internet as well as for the internet facing services;
l) ensure that access to VodafoneZiggo Information Systems for the Supplier to be able to support and monitor the respective services are documented, reviewed, and approved by VodafoneZiggo.

5.8 SECURITY LOGGING & MONITORING

Supplier shall:

a) define, document, implement and maintain security operating procedures including but not limited to the management of security event logging and monitoring. Supplier shall make these available to all users who need them, and shall review them on a regular periodic basis (at least once (1x) per calendar year) and update them as required in accordance with the state of the art and 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. Supplier shall follow up suspicious activities via a formal Security Incident management process;
c) effectively manage information security events and Security Incidents by establishing management responsibilities and procedures to support a quick, effective, and orderly response to information Security Incidents;
d) use knowledge gained from analysing and resolving information Security Incidents (types, volumes, and costs) to reduce the likelihood or impact of future Security Incidents;

e) where possible, define, document, implement and maintain procedures and supporting guidance for the identification, collection, acquisition and preservation of (log) data, which can serve as evidence, considering requirements of the relevant jurisdictions. Supplier shall review the procedures on a regular periodic basis (at least once (1x) per calendar year) and update them as required.

6 APPENDIX 1 – SECURITY INCIDENTS

6.1 URGENCY & IMPACT DEFINITIONS

The following table outlines the definitions of the Urgency & Impact of Security Incidents related to Products and Services provided by the Supplier:

Classification	Urgency description	Impact description
1 Critical	• The damage caused by the incident increases rapidly (impact doubles every 2hs); • Significant number of users are affected (90% users); • For significant data set the CIA is breached (90% data set); • For significant data set the CIA is breached (90% data set).	• Incident could cause extreme damage to the interests of VodafoneZiggo; • Very serious financial loss, severe loss of profitability or opportunity, grave embarrassment for VodafoneZiggo • Seriously damage to VodafoneZiggo brand(s) and/or reputation, and/or that of VodafoneZiggo customers or partners; • Breach of CIA for very significant data set and/or services.
2 High	• The damage caused by the incident increases considerable (impact doubles every 4hs); • Large number of customers impacted (> 75% users); • For a large data set the CIA is breached (> 75% data set); • A large data exfiltration is ongoing; (> 75% Data exfiltration).	• Incident could cause serious damage to the interests of VodafoneZiggo; • Serious financial loss, severe loss of profitability or opportunity, grave embarrassment for VodafoneZiggo; • Seriously damage to VodafoneZiggo brand(s) and/or reputation, and/or that of VodafoneZiggo customers or partners; • Breach of CIA for significant data set and/or services.

3 Medium	• The damage caused by the incident increases (impact doubles every 8hs); • Limited number of customers impacted. (> 50% users); • A limited number of Data Records are exfiltration (> 50% Data exfiltration);	• Incident could cause significant harm to the interests of VodafoneZiggo customers; • Financial loss, loss of profitability or opportunity, embarrassment or damage; • Brand and reputation and/or that of our customers or partners; • Breach of CIA for data set and/or services;
4 Low	Very limited number of Data Records impacted.	All other incidents

6.2 SECURITY INCIDENT PRIORITY LEVELS

The following table outlines the Incident Levels based on the Impact and Urgency of a Security Incident as defined in article 6.1 above.

	Urgency			
Impact	1 - Critical	2 - High	3 - Medium	4 - Low
1 - Critical	P0 - Crisis	P1 - Critical	P1 - Critical	P2 - High
2 - High	P1 - Critical	P2 - High	P2 - High	P3 - Medium
3 - Medium	P2 - High	P3 - Medium	P3 - Medium	P4 - Low
4 - Low	P2 - High	P4 - Low	P4 - Low	P4 - Low

Each incident priority level has its required response and resolution times. Additionally in case of P0, P1, or P2 priority Security Incidents, Supplier will deliver a Post Incident Report (PIR) to VodafoneZiggo. The table below defines the related response timelines.

Priority	7x24	Response time	Post Incident Report
P0	Yes	15 minutes	Within 1 working days
P1	Yes	15 minutes	Within 1 working days
P2	Yes	15 minutes	Within 2 working days
P3	No	30 minutes	Upon request
P4	No	1 hour	Upon request

7 APPENDIX 2 - VULNERABILITY, ISSUE AND PATCHING FIXING TIMELINES

Below timelines shall apply to all Products and/or Services impacted by the vulnerability, not only the original Product and/or Service for which the vulnerability was notified:

a) Emergency (Critical AND 'Zero day' OR actively exploited)
    a. Deploy following an emergency change process jointly agreed with involved Security teams as relevant, yet never exceeding 7 calendar days.
b) Critical (CVSS score 9.0-10.0):
    a. Deploy without undue delay, yet never exceeding 30 calendar days.
c) High risk (CVSS score 7.0-8.9):
    a. Internet-facing systems*: 30 calendar days
    b. Other systems: 90 calendar days
d) Medium risk (CVSS score 4.0-6.9):
    a. Internet-facing systems*: 90 calendar days
    b. Other systems: 180 days
e) Low risk (CVSS score 0.1-3.9): remediation by software updates; next lifecycle software update or release.

* Definition internet facing: 'means systems or applications that are reachable from the internet without needing to connect to an internal network via a VPN. Cloud assets which are accessible from the internet are to be considered internet.

8 APPENDIX 3 – SCREENING OF EXTERNALS

Where and as applicable, Supplier shall in accordance with the Dutch Regulation on safety and integrity telecommunication (*"Regeling veiligheid en integriteit telecommunicatie (RVIT)"*), requirement Category E.2 (Human Resource security)\, ensure and is required that Supplier personnel performing (particular) network management tasks (as stated in the RVIT) on behalf of VodafoneZiggo shall undergo a VOG screening as set out in chapter 2.4.b, section titled "Informatie" (translated "Information") of the VOG (Verklaring Omtrent Gedrag), June 2022.

This VOG screening assessment applies to the following three (3) categories:

Information*
Access to view and/or edit systems
Handling sensitive / confidential information
Access to information related to security systems, control mechanisms and verification processes

**For the purpose of this document, the official (Dutch) text in the VOG has been translated.*

For Supplier personnel located outside of the Netherlands and who are performing (particular) network management tasks (as stated in the RVIT), the Supplier shall ensure their personnel undergo equivalent screening in equivalent categories and extent as the VOG framework.