

Suppliers Security Requirements AGREEMENT

The "Agreement"

This Agreement is entered into between:

1. An Encevo Group company ENOVOS Luxembourg SA incorporated and existing under the laws of the Grand-Duchy of Luxembourg, having its registered office at 2 Domaine du Schlassgoard, L-4327 Esch-sur-Alzette, registered with the Luxembourg trade companies register under number B 44 683, hereby represented by Mustafa Öztuerk;

Hereinafter referred to as **"ENCEVO GROUP COMPANY"**

AND

2. [COMPANY NAME], having its registered office at [...], hereby represented by Mr [name] [title],

hereinafter referred to as the **"SUPPLIER"**,

the abovementioned ENCEVO GROUP COMPANY and the SUPPLIER are hereinafter individually referred to as a **"Party"** and collectively referred to as the **"Parties"**.

WHEREAS:

The Parties hereto have entered into a supplier agreement.

It is hereby agreed as follows based on the nature of relations, following chapters apply

	Chapter	Description
<input type="checkbox"/>	Limited access requirements	Only in case of limited access to Company Customer and PII via a user level access .
<input checked="" type="checkbox"/>	General security requirements	Applies if "Limited Access Requirements" part has not been advised as applicable.
Check what applies only if General security requirements is checked	<input type="checkbox"/> Security requirements for supplier staff	Only applies if staff is included in the execution of the agreement
	<input type="checkbox"/> Specificities in case of physical security on Encevo Group Company premises	Only applies if there is physical access to the Encevo Group Company premises
	<input checked="" type="checkbox"/> Specificities in case of provision of hosting environment or hosted services	Only applies if there is a hosting service or platform provided / managed by Supplier
	<input type="checkbox"/> Specificities in case of development of services	Only applies if there are development services provided to an Encevo Group Company
	<input type="checkbox"/> Specificities in case of access to Encevo Group Company systems	Only applies if there are (remote or on site) access to Encevo Group Company systems
	<input checked="" type="checkbox"/> Specificities in case of access to Encevo Group Company information on Supplier systems	Only applies if there are (remote or on site) access to Encevo Group Company information, hosted or processed on Supplier systems
	<input type="checkbox"/> Specificities in case of network assets support by supplier	Only applies for network support of Encevo Group Company on-prem assets
	<input type="checkbox"/> Specificities for protection of personal data	Only applies if Encevo Group Company PII data is concerned

DEFINITIONS

For the purposes of this Agreement the following terms are defined:

“Access” – the Processing, handling or storing Encevo Group Company Information by one or more of the following methods:

- interconnection with Encevo Group Company Systems
- Reception of paper or another non-electronic format
- Encevo Group Company Information on Supplier Systems
- Reception of mobile media
- Access to Encevo Group Company premises for the provision of the Supplies excluding the delivery of hardware and meeting attendance).

“Affiliated Company” means any corporation, firm, partnership or other entity which directly or indirectly controls or is controlled by or is under joint control with a Party (where control means in relation to a company the right to exercise a majority of the voting rights in that company).

“Authorised” - Encevo Group Company has approved Access either as part of Encevo Group Company's System Interconnect process or written authorisation has been received from the Encevo Group Company Security Contract . Access level provided will be relevant and limited to that required to provide the Supplies.

“Bulk Records” – means more than 1000 individual records of Encevo Group Company Information classified as In Confidence or 100 individual records of Encevo Group Company Information classified as In Strictest Confidence Note : The 1000 and 100 threshold level should not be taken into consideration when determining the severity of a security incident.

“Business Day” means a day of the year during which the Encevo Group subsidiaries are open for business in Luxembourg. **“Business Hours”** means any time of a Business Day between [8 AM CET] and [6 PM CET.]

“DPO” means Data Protection Officer;

“Encevo Group Company” means any legal entity belonging to the Encevo Group.

“Encevo Group Company Customer” – shall include for the purposes of these Security Requirements a corporate or individual to whom Encevo Group Company provides goods or services.

“Encevo Group Company Information” – all Information relating to Encevo Group Company or a Encevo Group Company Customer provided to the Supplier and all Information which is processed or handled by the Supplier on behalf Encevo Group Company or a Encevo Group Company Customer pursuant to the Contract.

“Encevo Group Company Confidential Information” means all business, technical, proprietary, trade secret, and other information, including information relating to intellectual property rights, that the disclosing Party (and its Affiliated Companies) discloses before or after the Effective Date in writing, orally, or in any other form, tangible or intangible; for the avoidance of doubt, Confidential Information might, but will not necessarily (i) bear the mention "Confidential" or a similar mention; or (ii) be communicated to the receiving Party with a specific statement to the end that such document or information is Confidential Information; for the avoidance of doubt, the Software (including the source code) and the corresponding Documentation constitute Confidential Information.

“Encevo Group Company Networks” - the network controlled or administered by Encevo Group Company.

“Encevo Group Company Physical Assets” - all physical assets (including but not limited to routers, switches, servers keys to cabinets, laptops tokens, pass cards, plans, or documentation) held by Supplier which belong to Encevo Group Company.

“Encevo Group Company Security” - the organisation defined within Encevo Group Company. To manage information security.

“Encevo Group Company Security Contact” – the information security professional within Encevo Group Company Security who will be the single point of contact for issues related to these Security Requirements and any Relevant Security Incident.

“Encevo Group Company Systems” – the services and service components, products, networks, servers, processes, paper-based system or IT systems (in whole or part) owned and/or operated by Encevo Group Company or other system that may be hosted on Encevo Group Company premises.

“Good Industry Security Practices” – means in relation to any undertaking and any circumstances, the implementation of the security practices, policies, standards and tooling which would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same type of activity under the same or similar circumstances.

“Information” – information whether in tangible or any other form, including, without limitation, specifications, reports, data, notes, documentation, drawings, software, computer outputs, designs, models, patterns, samples, inventions, (whether capable of being patented or not) and know-how, and the media (if any) upon which such information is supplied.

“Internal”, “Public”, “Restricted”, “Confidential” and “Secret” – have the meanings given to them in the Information Classification and Handling Specification.

“Network Assets”- device, or other component of the Encevo Group Company Network that supports network related activities.

“Network Security” - the security of the interconnecting communication paths and nodes that logically connect end user technologies together and associated management systems.

“Personal Data” means any information which are related to an identified or identifiable natural person either directly or indirectly especially by reference to an identifier such as a name, an identification number, location data, an online identifier or one of several special characteristics.

“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“Relevant Security Incident” - an observed or suspected security weaknesses in systems or services, and security events that affect the Supplies or the performance of the Contract (including actual or suspected loss, damage, theft or misuse of Encevo Group Company Information or Encevo Group Company Systems), including but not limited to:

- loss of service, equipment or facilities;
- corruption, damage or misuse of Encevo Group Company Physical Assets;
- system malfunctions or overloads;
- non-compliances with the security requirements described in this document;
- breaches of physical security arrangements;
- uncontrolled system changes;
- malfunctions of software or hardware;
- access violations; and
- known or suspected data losses or leakage related to systems associated with Encevo Group Company and the connection(s) between Encevo Group Company and Supplier.

“Remote Access” - remote access from home or another location via a public network (e.g. Internet) or Supplier network remotely access a Encevo Group Company System.

"Security Requirements" - means these Encevo Group Company security requirements as duly updated from time to time.

"Supplies" – shall mean any and all of the "Services", "Supplies" "Goods" and "Work" defined in the Contract and any performance of the Contract.

"Supplier Staff" "Relevant Supplier Staff" – exclusively external personnel as defined in the contract. It does not include visitors.

"Supplier Systems" – any Supplier owned computer, application or network systems used for accessing, storing or processing Encevo Group Company Information or involved in the provision of the Supplies.

"Supplier Security Contact" – such person whose contact information shall be notified by Supplier to Encevo Group Company from time to time who will be the single point of contact for issues related to these Security Requirements and any Relevant Security Incident.

"Transfer" or **"Transferred"** - the moving of Encevo Group Company Information in the possession of Supplier Staff (including, without limitation, Personal Data) from one location or person to another, whether by physical, voice or electronic means: and granting of Access to Encevo Group Company Information in the possession of Supplier Staff (including, without limitation, Personal Data) by one location or person to another, whether by physical, voice or electronic means.

1. Undertakings

INTRODUCTION

- This document sets out Encevo Group's security requirements.
- These Security Requirements are in addition to and without prejudice to any other obligations of the Supplier in the Contract (including, without limitation its obligations under the Conditions headed "Confidentiality", "Protection of Personal Data" and "Compliance").

LIMITED ACCESS REQUIREMENTS

This section will be advised as applicable where the Supplier will be providing **Supplies** that involve **limited access** to Encevo Group Company Customer and Personally Identifiable Information via a **user level access** to ENCEVO Group Company's Administrative Systems. Suppliers who fall into this category will not be required to comply with any other parts of this document.

1.1 Without prejudice to any obligations of confidentiality it may have, where the Supplier or Supplier Staff have access to Encevo Group (or subsidiary) Information, the Supplier shall:

- Ensure Encevo Group Company Information is not disclosed to or accessed by Supplier Staff unless necessary for the provision of the Supplies; and
- Put in place all systems and processes (both technical and organisational) as are required in accordance with Good Industry Security Practices to protect the security and confidentiality of Encevo Group (or subsidiary) Information and Systems.
- Ensure no remote support activity is performed from outside EU countries when Personal Data is involved. If not, it is mandatory to inform in the Encevo Group DPO concerned, put in place the Standard Contractual Clauses issued by the European Commission and any appropriate safeguards, as may deem necessary.

The Supplier must notify Encevo Group Company promptly and in any event within 2 working days when an employee, including contractors, temporary employees and agency workers, no longer require Access to Encevo Group Company systems, for example when employees leave or move roles.

GENERAL SECURITY REQUIREMENTS

Mandatory where "Limited Access Requirements" part has not been advised as applicable.

GENERAL INFORMATION SECURITY

1.1 The Supplier shall implement systems and processes (both technical and organisational) to:

- protect the security and confidentiality of Encevo Group Company Information and Systems as mandated in these Security Requirements; and
- ensure the availability, quality, integrity and adequate capacity to deliver the Supplies without interruption, as required by Good Industry Security Practice and following the agreed SLA/SLO requirements for the service.

1.2 The Supplier shall implement an IT change management process to ensure any changes to processes and Supplier Systems are implemented in a way that maintains the Supplier's compliance with these Security Requirements.

1.3 The Supplier shall make available to Encevo Group Company on written request copies of any security certifications and statement of compliance relevant to the Supplies in order to illustrate evidence of compliance with these Security Requirements.

- 1.4 The Supplier will take all reasonable steps to ensure appropriate individual(s) are appointed and made responsible as Point of Contact for Security and Incident Management. The Supplier shall notify Encevo Group Security Contact of the individual(s) Contact details and any change to them. Details should include:
 - name, responsibility, role and email address and/or telephone number
- 1.5 The Supplier shall, as a minimum annually or when there are any material changes to the Supplies or how they are provided, review the Security Requirements to ensure they are still compliant to all applicable Security Requirements.
- 1.6 If the Supplier subcontracts obligations under the Contract, then the Supplier shall ensure all contracts with relevant Subcontractors, include written terms requiring the Subcontractor to comply with Encevo Group's Supplier Security Requirements to the extent they are applicable, and inform the Encevo Group.
- 1.7 Unless explicitly required by Encevo Group Company, these terms must be in place between Supplier and its Subcontractor before the Subcontractor or any of its personnel can access Encevo Group Systems and information. The Supplier shall not sub-contract the treatment of Personal Data without the prior consent of the Encevo Group Company contracting party.

USE OF ENCEVO GROUP COMPANY INFORMATION

- 1.8 The Supplier shall not use Encevo Group Company Information for any purpose other than for the purpose for which it was provided to the Supplier and then only to the extent necessary to enable the Supplier to perform the Contract. Where the Supplier is Processing Personal Data, it shall not use any Personal Data which forms part of the Encevo Group Company Information for any purpose other than for the purpose specified in the relevant Contract.
- 1.9 Encevo Group Company Information may be retained for as long as necessary to execute the Contract, after which it should be retained **in any case no longer than a maximum of 3 months** unless a different retention period has been agreed between Encevo Group Company and Supplier or is required by any applicable laws. For the avoidance of doubt where the Supplier is Processing Personal Data, it shall not retain any Personal Data which forms part of the Encevo Group Company Information for longer than the periods specified in the Condition headed "Protection of Personal Data".

INFORMATION HANDLING

- 1.10 The Supplier shall have and follow information handling which as minimum shall ensure the Supplier:
 - 1.10.1 implements appropriate processes to prevent the unauthorised distribution of Encevo Group Company Information in any form and by any way, including by email, fax, social media, print or post (e.g. a clear desk and screen policy in place, Secret Information not sent by email...);
 - 1.10.2 does not discuss Encevo Group Company Information in meetings unless all attendees are:
 - (i) authorised to attend the meeting;
 - (ii) need to know the information being discussed; and
 - (iii) are aware of, and consider, their confidentiality obligations;
 - 1.10.3 does not store Encevo Group Company Information:
 - in the cloud or with internet services including, but not limited to, Google Docs, GitHub, Dropbox, Pastebin or Facebook unless agreed in writing with Encevo Group Company;
 - on any laptop or other device unless it is protected with a full disk encryption feature (such as BitLocker) that meets the standards mentioned below in the paragraph "encryption"; or
 - 1.10.4 deletes or puts Encevo Group Company Information beyond use of daily business activities in a secure manner.
 - 1.10.5 maintains a clear-desk and a clear-screen policy to protect Encevo Group Company Information.

INFORMATION BACKUP

1.11 The Supplier commits to:

- 1.11.1 perform backups of the data entrusted to it by the Client or to which it may have access in the context of the performance of this Agreement;
- 1.11.2 ensure backups are kept on separate tapes/drives than data belonging to or accessed by other companies.
- 1.11.3 encrypt backups with Storage Encryption that ideally accommodates key escrow by Supplier
- 1.11.4 physically secure Backup media against theft or tampering.
- 1.11.5 ensure that all backup media is tracked and must ensure that contractual data destruction requirements can be met.

TRANSMISSION OF DATA

- 1.12 Transmission of Encevo Group Company Information should be exclusively made via an Encevo Group Company approved transfer platform.

ENCRYPTION

- 1.13 The Supplier shall ensure Encevo Group Company Information is encrypted both at rest and in transit, in accordance with Good Industry Security Practice ensuring that standards deprecated by the relevant industry are not used.

INCIDENT HANDLING

- 1.14 If Encevo Group Company has reason to suspect that there has been a:

- Personal Data Breach as defined under GDPR ;
- Relevant Security Incident.

Encevo Group Company shall inform the Supplier Security Contact and the Supplier agrees, at its own cost:

- to take action immediately to investigate the suspected breach and to identify, prevent and make reasonable efforts to mitigate the effects of any such breach; and
- to carry out any recovery or other action necessary to remedy the breach.
- provide to Encevo Group Company such reports as Encevo Group Company shall reasonably require concerning the investigation findings and actions taken to remedy or mitigate the breach,

- 1.15 In the event of a Personal Data breach and/or Relevant Security Incident, Supplier shall fully cooperate with Encevo Group Company in any ensuing investigation or audit by Encevo Group Company, an external party mandated by Encevo Group Company, a regulatory authority and/or any law enforcement agency, such investigation or audit to include (upon reasonable notice by Encevo Group Company to the Supplier) access to Encevo Group Company Information held within Supplier's premises or on Supplier Systems

- 1.16 The Supplier shall have and shall follow a formal security incident management process which includes defined responsibilities for addressing a Relevant Security Incident. Any information related to a Relevant Security Incident shall be treated "In Confidence".

- 1.17 The Supplier shall inform the Encevo Group Company Security Contact, within a reasonable period of time upon its becoming aware of any Relevant Security Incident as defined under the Annex "Definitions", and in any event, no later than twelve (12) hours from the time the Relevant Security Incident comes to the Supplier's attention.

- 1.18 Without unreasonable delay, the Supplier shall promptly take appropriate and timely corrective action to mitigate any risks and effects related to the Relevant Security Incident in order to reduce the severity and duration of the incident.

- 1.19 The Supplier agrees to provide all information reasonably required by Encevo Group Company in respect of a Relevant Security Incident including but not limited to the:
- date and time;
 - location;
 - type of incident;
 - impact;
 - classification of information impacted;
 - status; and
 - outcome (including the resolution recommendations or actions taken).
- 1.20 The Supplier shall ensure that identified risks as to the confidentiality, integrity or availability of Encevo Group Company Information in the Supplier's processes or Supplier Systems, are promptly remedied.
- 1.21 If a Relevant Security Incident occurs, then the Supplier shall promptly notify the Encevo Group Company Security Contact and the DPO of any technical, organisational or other incidents (including incidents at Sub-processors), which have resulted or may result in a Personal Data Breach. This notification shall be accompanied by all relevant and comprehensive documentation and the Supplier shall provide assistance to the Encevo Group Company concerned before the Supervisory authority, as may be necessary. . For the avoidance of doubt , this paragraph remains applicable in respect of any Personal Data Breach notwithstanding the fact that the breach may, or may not be, a Relevant Security Incident

AUDIT & SECURITY REVIEW

- 1.22 Without prejudice to any other right of audit that Encevo Group Company may have, in order to assess the Supplier's compliance of these Security Requirements and where applicable the Security Requirement headed "Protection of Personal Data", Encevo Group Company or its appointed representatives reserves the right to conduct a security compliance audit from time to time, on any or all aspects of the Supplier's policies, processes and system(s) by a document based security review.

SECURITY REQUIREMENTS FOR SUPPLIER STAFF

- 1.1 Supplier shall ensure that concerned Staff have signed and/or are bound by confidentiality agreements before starting to work in Encevo Group Company buildings or on Encevo Group Company Systems or have access to Encevo Group Company Information. These confidentiality agreements must be retained by Supplier.
- 1.2 The Supplier staff shall deal with breaches of Supplier's and Encevo Group Company's security policies and procedures, through formal processes including action which may include removal of the individual from:
- having access to Encevo Group Company Systems or Encevo Group Company Information;
 - or
 - carrying out work connected with the provision of the Supplies.
- 1.3 Supplier should ensure they have relevant processes in place to ensure any Supplier Staff who have been so removed are not subsequently given access to Encevo Group Company Systems, Encevo Group Company Information or allowed to work in connection with the provision of the Supplies.
- 1.4 When Supplier Staff are no longer assigned to the Supplies, the Supplier shall ensure that:
- access to Encevo Group Company Information is revoked; and
 - at Encevo Group Company's option, any Encevo Group Company Physical Assets or Encevo Group Company Information in the possession of Supplier Staff should be handed back to the relevant Encevo Group Company operational team; or destroyed.
- 1.5 Unless otherwise agreed in writing with the Encevo Group Company Security Contact, the Supplier shall implement a controlled exit procedure for Supplier Staff which includes the written request to the Encevo Group Company Security Contact for the removal of access to Encevo Group Company Systems, Encevo Group Company Information, and all other Access and accesses. Supplier Staff

should be advised that their confidentiality agreement will remain in force and that Encevo Group Company Information acquired through work on the Supplies must not be disclosed.

- 1.6 As part of the granting of Access the Supplier shall maintain and supply records of all Supplier Staff that require access or are involved in the provision of Supplies to Encevo Group Company, (including their name, location they work in, business e-mail address, User Id requested (If they have one), date they were assigned to the provision of Supplies to Encevo Group Company, date they cease providing Supplies).
- 1.7 Supplier Security Contact should ensure at all time that only Supplier Staff are Authorised.

SPECIFICITIES IN CASE OF PHYSICAL SECURITY ON ENCEVO GROUP COMPANY PREMISES

- 1.1 By default, Contract Personnel is not provided with a permanent or limited duration electronic access card. However, it may be provided in accordance with local issuance instructions.
- 1.2 Where Contract Personnel have been issued with an Authorised Access Card by Encevo Group Company the Supplier must notify Encevo Group Company promptly and in any case within 2 working days when such Supplier Staff no longer requires access to Encevo Group Company premises.
- 1.3 Only approved Encevo Group Company build servers, Encevo Group Company PCs and Trusted End Devices are allowed to directly connect (plug into LAN port or Wireless connection) to Encevo Group Company domains. Supplier shall not (and, where relevant, shall ensure that any Supplier Staff shall not) without the prior written authorisation of the Encevo Group Company Security Contact connect any equipment not approved by Encevo Group Company to any Encevo Group Company Domain. In any event Supplier must ensure that no equipment personally owned by Supplier Staff or any other employees, (including contractors, temporary employees and agency workers) is used to store, access or process any Encevo Group Company data.
- 1.4 No Encevo Group Company Information shall be removed from Encevo Group Company premises and no equipment or software shall be either removed or installed in Encevo Group Company Premises without prior authorisation by Encevo Group Company.
- 1.5 Supplier shall ensure that photography and/or the image capture of any Encevo Group Company Information or Encevo Group Company Customer information (including Personal Data) is prohibited. Under exceptional circumstances where there may be business requirements to capture such images, temporary exemption to this provision must be obtained in writing from the Encevo Group Company Security Contact.

SPECIFICITIES IN CASE OF PROVISION OF HOSTING ENVIRONMENT OR HOSTED SERVICES

Compliance with this section is required if the Supplier is providing a hosting environment for Encevo Group Company.

ACCESS CONTROL

- 1.1 The Supplier shall maintain access controls on Supplier Systems appropriate to the environment and nature of the Supplies supplied to Encevo Group Company ensuring where applicable that:
 - all users, including administrator level users, have unique ID's;
 - regular password changes are required;
 - appropriate protections are implemented following unsuccessful login attempts to prevent brute force attacks;
 - unused accounts are automatically disabled;

- passwords of an appropriate strength (with a minimum of 10 characters requirement incorporating three of the following categories: (i) upper case; (ii) lower case; (iii) numeric; and (iv) non-alpha numeric) are used and password history is enforced to prohibit the use of previous passwords within a 12 month period;
- role-based access to Supplier Systems is implemented with as a minimum more stringent access controls for administrator access; and
- regular reviews and audits of user access are undertaken.

REMOTE ACCESS

- 1.2 The Supplier is not permitted to allow Supplier Staff to Remote Access information classified as "Secret" or to Personal Data unless otherwise agreed with Encevo Group Company in writing. Where Remote Access is permitted, the Supplier shall ensure that Remote Access is subject to appropriate security controls within Supplier's organisation, including but not limited to ensuring Remote Access by users being subject to strong two factor authentication.
- 1.3 If Remote Access via public networks for support purposes is utilised, the connections will be encrypted in accordance with the standards of set out in paragraph "Encryption".

PATCHING

- 1.4 The Supplier shall have and follow a documented patch management process which as a minimum shall ensure that the Supplier:

- Deploy patches within the following timeframes:

Patch Type	Description	Timeframe
Critical patches	Patches necessary to address zero-day vulnerabilities	As soon as practicable and in any event within 30 days of a patch becoming available
Important patches	Vulnerabilities classified as High 7.0 -8.9 on the qualitative severity rating scale from the Common Vulnerability Scoring System (CVSS)	Within 60 days of a patch becoming available

- monitors all applicable vendors for patch releases.
 - uses patches obtained from: vendors directly for proprietary systems and patches that are either (i) digitally signed or (ii) verified via the use of a vendor hash for the update package such that the patch can be identified as coming from a reputable support community for open source software;
 - tests all patches on systems that accurately represent the configuration of the target production systems before deployment of the patch to production systems and that the correct operation of the patched service is verified after any patching activity; and
 - maintains and updates Supplier Systems to ensure the most up to date vendor patches can be applied.
- 1.5 If a system cannot be patched by the Supplier, the Supplier must notify Encevo Group Company in writing. On receipt of such a notification, Encevo Group Company shall review the risk to Encevo Group Company and Encevo Group Company Information associated with the continued use by the Supplier of the system and Encevo Group Company may require the Supplier to undertake any reasonable steps (at the Supplier's cost) to address any such risks.

VULNERABILITY MANAGEMENT

1.6 The Supplier shall have and follow a vulnerability management process which as a minimum shall ensure that the Supplier:

- takes appropriate actions (for example scanning) to identify vulnerabilities;
- undertakes its own regular penetration testing; and maintains reports of such testing; and
- reacts to any notification of vulnerabilities and implements action plans to mitigate known vulnerabilities in accordance with paragraph related to Threat Management and Incident Handling.

PEN TESTING

1.7 The Supplier shall:

- permit Encevo Group Company (or authorised Encevo Group Company subcontractors) to carry out reasonable penetration testing on reasonable notice; and
- provide Encevo Group Company access to existing Supplier penetration test reports relevant to the Supplies being provided.

AUDIT AND LOGGING

1.8 The Supplier shall have and shall follow an audit and logging process which as a minimum shall ensure that the Supplier logs (as appropriate) the following events:

- the start and stop points of the logged process;
- changes to the type of logged events as required by the audit trail (for example the start-up parameters and any changes to them);
- Supplier System start-up and shut-down;
- successful logins;
- failed login attempts (for example wrong user ID or password);
- all operations performed by privileged users (for example users with powerful access to system utilities or applications);
- successful and unsuccessful privilege escalation;
- all access by the Supplier or Supplier Staff to or operations on In Strictest Confidence Information; and
- creation, modification and deletion to/of user accounts.

1.9 For each auditable event, the Supplier shall maintain a tamper proof audit trail that enable the reconstruction of such events.

1.10 Taking into account the criticality of the component/data, the Supplier shall regularly inspect and analyse audit logs to detect suspicious or anomalous behaviour and take appropriate action and/or raise an alarm.

1.11 All alarms must be documented and acted upon in a timely manner determined by the criticality of the alarm.

1.12 Supplier shall retain all log files for 3 months (unless other required to delete these pursuant to the Condition headed "Protection of Personal Data") and shall produce copies or permit access to the logs files at Encevo Group Company's request in an exploitable / structured digital format agreed by both Parties.

CLOUD SECURITY

Compliance to the clauses in this section is required when the Supplier is providing Encevo Group Company with **Cloud services**.

1.13 The Supplier shall comply with the latest version of the Cloud Security Alliance Cloud Controls Matrix (CCM);

- 1.14 Supplier shall, implement security measures across all supplied components, such that it safeguards the confidentiality, availability, quality and integrity of the Supplies by minimizing the opportunity of unauthorised individuals (e.g. other cloud customers) from gaining access to Encevo Group Company Information, and Encevo Group Company Supplies.
- 1.15 Upon request by Customer made within 30 days after the request effective date, Supplier will make Customer Data available to Customer for export or download as provided in the Documentation.

SPECIFICITIES IN CASE OF DEVELOPMENT OF SERVICES

Compliance with this section is required if Supplier is dealing with the development of Supplies for use by Encevo Group Company and/or Encevo Group Company Customers. This includes “components off the shelf”, configuration of software and manufacturing components for the Supplies.

INTELLECTUAL PROPERTY

- 1.1 Supplier shall own all rights, in particular intellectual property rights (“IP rights”) which are necessary for the development of Supplies and shall be entitled to grant the licence/right to use of such IP rights in favor of the Encevo Group Company under conditions of the Contract.
- 1.2 Supplier shall have obtained the rights to use of any third-party products necessary to enable the development of the Supplies to operate in accordance with the specifications, and to allow the Encevo Group Company to benefit from such rights;
- 1.3 Supplier shall, implement agreed security measures across all supplied components that constitute the Supplies and/or Services, such that it safeguards the confidentiality, availability and integrity of the Supplies, including by:
 - maintaining appropriate documentation in relation to the implementation of security in accordance with best industry practice;
 - minimising the opportunity for unauthorised individuals (e.g. hackers) to gain access to Encevo Group Company Systems and Encevo Group Company Information, Encevo Group Company Networks or Encevo Group Company Supplies; and
 - minimising the risk of misuse of Encevo Group Company Systems and Encevo Group Company Information, Encevo Group Company Networks or the Services which could potentially cause loss of revenue or service.

CONFIGURATION HARDENING

- 1.4 Supplier shall ensure that the development of systems for use by Encevo Group Company or the build and maintenance of Encevo Group Company owned hardware is hardened following the Encevo Group Company's IT Security Requirements if provided. If not provided requirements are aligned on the best industry practices (e.g. Owasp recommendations, ANSSI documents, NIST publications...).

ENVIRONMENT SEGREGATION

- 1.5 Supplier shall ensure that systems and processes used for test and development activities are segregated from production systems. A change control process must be used for the promotion of any code to the production environment. Encevo Group Company provided test data must be deleted after a period determined by the Encevo Group Company data owner (and in any case no longer than the end of the contract) and no live or production data can be used in development or test environments.

SECURITY VULNERABILITIES AND PEN TESTS

- 1.6 All critical security vulnerabilities found in security testing and classified as medium risk or above must be fixed prior to release. Any security weaknesses in the Services identified by Encevo Group Company or the Supplier shall be remedied at the Supplier's cost within such timescales as Encevo Group Company shall reasonably require.

- 1.7 The Supplies must be subject to independent penetration testing commissioned by the Supplier prior to release and following major changes or incidents at Supplier's own cost.

SECURE DEVELOPMENT LIFECYCLE

- 1.8 Supplies developed for use by Encevo Group Company or its customers must be developed using a documented, recognised industry standard Secure Development LifeCycle (SDLC) to minimise the risk of introducing security vulnerabilities into the production environment and/or to customers. The SDLC must include the following gates, with tangible artefacts resulting from each review and available for inspection by Encevo Group Company within the audit framework at paragraph 5 of Part 3 of these Security Requirements:

- security review of the business requirements;
- security review of the design;
- security review of the source code – automatic and/or manual; and
- security audit of the solution prior to deployment (to include simulated attacks) according to a documented, project-specific audit plan based on the reports resulting from the security reviews of business requirements, design and code.

It is then recommended to follow the ISO5055 standard (ISO/IEC 5055) that provides engineering rules for finding and preventing critical flaws, and can be used to assess the internals of software systems on four business-critical factors – Security, Reliability, Maintainability, Performance Efficiency.

SPECIFICITIES IN CASE OF ACCESS TO ENCEVO GROUP COMPANY SYSTEMS

Compliance with this section is required if Supplier Staff need to access Encevo Group Company Systems in order to provide Supplies.

- 1.1 Encevo Group Company may allow, at its sole discretion, limited Access as is strictly necessary for the provision of Supplies.
- 1.2 In relation to Access, Supplier shall adhere to all relevant Encevo Group Company policies, standards and instructions provided to Supplier, and shall:
- ensure user identification, passwords, PINs, tokens, and conferencing access are for **individual** Supplier Staff and **not shared**. Details must be stored securely and separately from the device they are used to access. If a password is known by another person, it must be changed immediately;
 - on reasonable request, provide to Encevo Group Company reports as e.g. Supplier Staff Authorised to access Encevo Group Company Systems;
 - ensure inter-domain linking to Encevo Group Company Systems (i.e. connecting Supplier system to Encevo Group Company one) is not possible unless specifically approved and authorised by Encevo Group Company Security Contact;
 - use all reasonable endeavours to ensure no viruses or malicious codes are introduced to minimise risk of corruption to Encevo Group Company Systems or Encevo Group Company Information through any means whatsoever;
 - use reasonable endeavours to ensure that files which contain information, data or media with no relevance to the Supplies are not stored on Encevo Group Company Equipment, Encevo Group Company servers, Encevo Group Company provided laptops and desktops, Encevo Group Company centralised storage facilities or Encevo Group Company Systems.
 - where Encevo Group Company has provided Supplier with access to the internet or Encevo Group Company's intranet, ensure that the Supplier Staff only access the internet or Encevo Group Company intranet appropriately and only enable them to provide the applicable Supplies and that unacceptable or dangerous sites should be blocked from the user.

- 1.3 The Supplier must carry out regular reviews to ensure that Access is required to perform the role. Copies of review documentation must be made available for inspection by Encevo Group Company within the audit framework described in paragraph 5.1:

SPECIFICITIES IN CASE OF ACCESS TO ENCEVO GROUP COMPANY INFORMATION ON SUPPLIER SYSTEMS

Compliance with this section is required if Encevo Group Company Information is being stored or processed on Supplier Systems.

- 1.1 If Supplier Staff are granted Access to Supplier Systems for the purpose of providing the Supplies and/or Services, the Supplier shall demonstrate accountability for such Access (including, but not limited to the use of unique user accounts, password management and a clear audit/log trail for all Supplier Staff action)
- 1.2 Supplier shall maintain systems which detect and record any attempted damage, modification or unauthorised access to Encevo Group Company Information on Supplier Systems.
- 1.3 Supplier shall maintain controls to detect and protect against malicious software, viruses and malicious codes on Supplier Systems and ensure that appropriate user awareness procedures are implemented.
- 1.4 Supplier shall ensure that any unauthorised software is identified and removed from Supplier Systems holding, processing or accessing Encevo Group Company Information at least monthly.
- 1.5 Supplier shall ensure that access to diagnostic and management ports as well as diagnostic tools are securely controlled.
- 1.6 Supplier shall ensure that access to Supplier's audit tools are restricted to Supplier Staff and their use is monitored.
- 1.7 Supplier shall ensure code reviews and penetration testing on all in-house produced software (including any Software) used to process Encevo Group Company Information is performed by an independent team that must not include the developers of the software.
- 1.8 To the extent that any servers are used to provide the Supplies, they must not be deployed on untrusted networks (network's outside your security perimeter, that are beyond your administrative control e.g., internet-facing) without appropriate security controls.
- 1.9 Supplier shall ensure that changes to individual Supplier Systems which hold and process Encevo Group Company Information and/or which are used to provide the Supplies, are controlled and subject to formal change control procedures.
- 1.10 Supplier shall ensure that all system clocks and times are synchronised using the latest version of NTP or a similar time synchronisation technology.
- 1.11 Additional levels of authentication (Multifactor...) may be required based on the sensitivity of the data and functionality to be accessed.

SPECIFICITIES IN CASE OF NETWORK ASSETS SUPPORT BY SUPPLIER

Compliance with this section is required where the Supplier is building, developing or supporting Encevo Group Company Networks or Network Assets.

- 1.1 The Supplier shall, in relation to the Supplies, implement agreed security measures across all supplied components, such that it

- safeguards the confidentiality, availability and integrity of the Encevo Group Company Networks and/or assets.
 - ensure that all Network Security for which the Supplier is responsible meets all legal and regulatory requirements; and
 - uses its best endeavours to prevent unauthorised individuals (e.g. hackers) from gaining access to the Network Management Elements and other elements accessed via the Encevo Group Company Networks; and
 - uses its best endeavours to reduce the risk of misuse of the Encevo Group Company Networks and/or by those individuals authorised to access it, which could potentially cause loss of revenue or service; and
 - uses its best endeavours to detect any security breaches that might occur ensuring quick rectification of any breaches, alongside the identification of the individuals who obtained access and determination of how they obtained it; and
 - minimise the risk of misconfiguration of Encevo Group Company Networks for example by granting the minimum permissions required to fulfil the contracted role.
- 1.2 The Supplier must take all reasonable steps to secure all interfaces on the Supplies and/or Services and should not assume that the supplied components are operated in a secure environment.
- 1.3 The Supplier shall provide to the Encevo Group Company Security Contact the names, addresses (and such other details as Encevo Group Company shall require) of all individual Supplier Staff who shall from time to time be directly involved in the deployment, maintenance and/or management of the Supplies before they are respectively engaged in such deployment, maintenance and/or management.
- 1.4 The Supplier shall provide the Encevo Group Company Security Contact with a schedule (updated as necessary from time) of all active components comprised in the Supplies and/or the Services and their respective sources.
- 1.5 The Supplier shall provide details of its individual personnel who will liaise with the Encevo Group Company vulnerability management (CERT) team in relation to discussion around Encevo Group Company and Supplier-identified vulnerabilities in the Supplies and/or Services. The Supplier shall provide Encevo Group Company with timely information on vulnerabilities, and comply (at the Supplier's cost) with such reasonable requirements in relation to vulnerabilities as may be notified by the Encevo Group Company Security Contact from time to time. The Supplier shall inform Encevo Group Company of any vulnerabilities in sufficient time to allow mitigating controls to be applied or installed ahead of the Supplier releasing the vulnerabilities publicly.
- 1.6 The Supplier must not use any network monitoring tools that can view application information.
- 1.7 The Supplier shall maintain hardware and software according to manufacturers' specifications.

SPECIFICITIES FOR PROTECTION OF PERSONAL DATA

Compliance to the requirements in this section is required when the purpose of the Contract is or incorporates processing of Personal Data. Capitalized terms used in this paragraph are those defined under the "DATA PROCESSING APPENDIX" (the "DPA").

- 1.1 The Parties shall comply with European regulations and national laws governing the treatment of personal data (hereafter defined the "Law"), in particular the European Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (hereinafter referred to as the "GDPR").
- 1.2 As defined by the GDPR, when the Encevo Group Company acts as a Data Controller, the Supplier may act either as Data Processor or as Data Controller or joined Data Controller in the treatment of the Personal Data of the Data Subjects. The Supplier shall process the Personal Data only for the purposes defined by the Parties and in compliance with the Law, notably in accordance with the provisions of articles 28 and 32 of the GDPR.

- 1.3 When the Supplier is acting as Data Processor, the DPA shall be completed and inserted as an appendix to the Contract. The Supplier undertakes to comply with the obligations further detailed in the DPA
- 1.4 In the event of failure, breach or non-compliance of the obligations prescribed by the GDPR or of the provisions provided by the DPA and notwithstanding anything to the contrary in the Contract, the Supplier shall remain fully liable of any damage, including any damage caused by any of its employee, any person under its direction, authority, control, liability or acting on its behalf.

SIGNATURE**FOR THE SUPPLIER** (For and on behalf of)

DATE:

DATE: