ENCODE A/S

SECURITY AND INFRASTRUCTURE POLICY

(Revision March 2021)

This Encode Software as a Service ("SaaS") Security and Infrastructure Policy applies to the Service provided by Encode as part of the SaaS offering acquired by the Customer under the Customer's ordering document. This Policy is subject to change at Encode's discretion.

This policy describes the architecture of, the security-and-privacy-related audits and certifications received for, and the administrative, technical and physical controls applicable to Encode Software as a Service ("SaaS").

1. SECURITY ASSESSMENTS AND COMPLIANCE

1.1 Data Centres

Encode's physical infrastructure is hosted and managed within Google Cloud's and Amazon Web Services (AWS) secure data centers. Encode's default point of delivery is from within Google Cloud. In specific cases, the Customer and Encode can agree to use AWS instead - such agreement will be stated in the Customer Order Form. Google (and Amazon) continually manage risk and undergo recurring assessments to ensure compliance with industry standards. AWS's and Google's data centre operations have been accredited under:

- ISO 27002
- ISO 27017
- A full list of Google Cloud Platform accreditations can be accessed at https://cloud.google.com/security/compliance/#/.
- A full list of AWS accreditations can be accessed at https://aws.amazon.com/compliance/programs/.

2. PENETRATION TESTING AND VULNERABILITY ASSESSMENTS

Encode performs regular penetration and vulnerability testing. Independent and reputable security consulting firms conduct third-party security testing of the Encode Service. The Customer has the right to choose a third-party firm to perform its own additional audit once Encode has authorised approval. Findings from each assessment are reviewed with the assessors, risk ranked and assigned to the responsible team.

Encode utilises ISO 27001 certified data centers managed by Google (and AWS).

Google and AWS design and build their own data centres, which incorporate multiple layers of physical security protections. Access to these data centres is limited to only a very small fraction of AWS and Google employees. AWS and

Google use multiple physical security layers to protect their data centre floors and use technologies like biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection systems.

A full description of the Google Cloud Platform (GCP) environment can be accessed at https://cloud.google.com/security/infrastructure/design/.

A full description of the AWS environment can be accessed at https://aws.amazon.com/security/.

3. NETWORK SECURITY

3.1 Firewalls

Firewalls are utilised to restrict access to systems from external networks and between systems internally. By default, all access is denied, and only explicitly allowed ports and protocols are allowed based on business needs. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk. Recording of all activity is undertaken and stored within logs for scrutiny.

3.2 Denial of Service (DoS) Protection

3.2.1 AWS

Encode deploys AWS Shield Standard as a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS.

A full description of AWS Shield can be accessed at https://aws.amazon.com/shield/.

3.2.2 Google Cloud Platform

Encode deploys GCP Cloud Armor Standard as a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on GCP.

A full description of GCP Cloud Armor can be accessed at https://cloud.google.com/armor.

Encode works closely with our providers to quickly respond to events and enable advanced DoS mitigation controls when needed.

3.3 Port Scanning

Port scanning is prohibited. When port scans are detected, they are stopped, and access is blocked.

3.4 Anti-malware

Anti-malware protection is in place on all personal computing devices used at any time to store or process Customer Data, and a process for dealing with actual or suspected malware infections is in place.

4. DATA SECURITY AND SEGREGATION

4.1 Customer Data

Each Customer on the Encode platform runs within its own isolated environment and cannot interact with other applications or areas of the system. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and files.

The Encode SaaS is operated in an architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific "Organisation IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the “Authorised sub-processors” documentation available in the Encode Data Processing Agreement (“DPA”).

4.2 Customer Storage and Disposal

Encode ensures that all Customer Data held either logically or physically by them is secured appropriately and destroyed when no longer required either through shredding or incineration for paper-based assets or through EU Waste Electrical and Electronic Equipment (WEEE) regulation aligned methods for electronic information.

A full description of the AWS and Google Cloud Platform controls for media destruction can be accessed at :

https://aws.amazon.com/compliance/data-center/controls/
https://cloud.google.com/security/deletion

4.3 Control of Processing

Encode has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Encode and its subprocessors. In particular, Encode and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organisational data security measures implemented by Encode and its sub-processors are subject to regular audits. The “Infrastructure and

Sub-processors" documentation describes the subprocessors and certain other entities material to Encode's provision of the Software-as-a-Service.

4.4 Sensitive Data

The following types of sensitive personal data may not be submitted to the Encode SaaS: financial information (such as credit or debit card numbers, bank account numbers, personal health information, and any related security codes or passwords).

If the Customer does submit personal health information or other sensitive or regulated data to Encode SaaS, then Customer is responsible for ensuring that its use of the Encode SaaS to process that information complies with all applicable laws and regulations.

For clarity, the foregoing restrictions do not apply to financial information provided to Encode for the purposes of checking the financial qualifications of, and collecting payments from, its customers.

5. SYSTEM SECURITY

5.1 System Configuration

System configuration is maintained through a secure source control system, which through automated pipelines ensure new systems and system upgrades are done in a secure, tested and repeatable way. In case of a disaster recovery scenario, configuration is used to recreate the system with exact same configuration at a new data center.

5.2 System Authentication

Operating system access is limited to Encode staff and requires two-factor authentication. Operating systems do not allow password authentication to prevent password brute force attacks, theft, and sharing.

6. VULNERABILITY MANAGEMENT

Encode's vulnerability management process is designed to remediate risks without customer interaction or impact. Encode is notified of vulnerabilities through internal and external assessments, system patch monitoring, and third-party mailing lists and services. Each vulnerability is reviewed to determine if it applies to Encode's environment, ranked based on risk, and assigned to the appropriate team for resolution.

New systems are deployed with the latest updates, security fixes, and Encode configurations, and existing systems are decommissioned as customers are migrated to the new instances. This process allows Encode to keep the environment up-to-date. Since customer applications run in isolated environments, they are unaffected by these core system updates.

To further mitigate risk, each component type is assigned to a unique network security group. These security groups are designed to only allow access to the ports and protocols required for the specific component type.

All patches are tested and approved before deployment within a system of record.

7. INCIDENT MANAGEMENT

Encode maintains security incident management policies and procedures. Encode notifies impacted customers without undue delay of any unauthorised disclosure of their respective Customer Data by Encode or its agents of which Encode becomes aware to the extent permitted by law. Encode typically notifies customers of significant system incidents by email, and for incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Encode's response.

Encode will provide the Customer with such assistance and co-operation as the Customer may request in relation to the conduct of investigations which includes the preserving of any evidence if required for forensic analysis.

8. DISASTER RECOVERY

Disaster recovery services are intended to provide service restoration capability in the case of a major disaster, as declared by Encode, that leads to loss of a data centre, loss of data, and corresponding service unavailability.

For the purposes of this Policy, a "disaster" means an unplanned event or condition that causes a complete loss of access to the primary site used to provide the Encode SaaS such that the Customer production environments at the primary site are not available.

Encode is committed to minimising downtime due to any disasters or equipment failures. As part of this commitment, Encode has a corporate business disaster recovery plan for a timely recovery and restoration of Encode operations, compiled to reflect the industry best practice standard ISO 22301:2019.

8.1 System Resilience

Encode SaaS maintains a redundant and resilient infrastructure designed to maintain high levels of availability and to recover services in the event of a significant disaster or disruption. Encode designs the SaaS platform using principles of redundancy and fault-tolerance with a goal of fault-tolerance of a single node hardware failure.

Encode SaaS provides an infrastructure that incorporates a comprehensive data backup strategy. Encode has one data centre that functions as the primary site for Encode SaaS. The Customer's disaster recovery site (secondary site) environment will reside in a data centre separate from the Customer's primary site. Encode will commence the disaster recovery plan under this Policy upon its declaration of a disaster, and will target to recover the production data and

use reasonable efforts to re-establish the production environment at the secondary site.

Encode provides for the recovery and reconstitution of its production SaaS to the most recently available state following a disaster. Encode reserves the right to determine when to activate the Disaster Recovery Plan. During the execution of the Disaster Recovery Plan, Encode provides regular status updates to Customers.

Note: the RTO and RPO described below do not apply to Customer customisations that depend on external components or third-party software. During an active failover event, non-critical fixes and enhancement requests are not supported. Customer will be solely responsible for issues arising from third-party software, customisations to Encode services, and updating allow lists if required.

8.2 Recovery Time Objective

Recovery time objective (RTO) is Encode's objective for the maximum period of time between Encode's decision to activate the recovery processes under this Policy to failover the service to the secondary site due to a declared disaster, and the point at which Customer can resume production operations in the standby production environment. If the decision to failover is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade. The RTO is 4 hours from the declaration of a disaster.

8.3 Recovery Point Objective

Recovery point objective (RPO) is Encode's objective for the maximum possible length of time during which data could be lost, in the event of a disaster. The RPO is 2 hours from the occurrence of a disaster, excluding any data loads that may be underway when the disaster occurs.

8.4 Approvals and Reviews

This Policy and the corresponding Disaster Recovery Plan is reviewed annually. The Plan is revised during the review process to incorporate problem resolutions and process improvements.

8.5 Disaster Recovery Plan Objectives

The following are the objectives of Encode's Disaster Recovery Plan for Encode SaaS:

- In an emergency, Encode's top priority and objective is human health and safety.
- Maximise the effectiveness of contingency operations through the established Disaster Recovery Plan that consists of the following phases:

- Phase 1 - Disaster Recovery Launch Authorisation phase - to detect service disruption or outage at the primary site, determine the extent of the damage and activate the plan.
- Phase 2 - Recovery phase - to restore temporary IT operations at the secondary site.
- Phase 3 - Reconstitution phase - to restore processing capabilities and resume operations at the primary site.

- Identify the activities, resources, and procedures to carry out processing requirements during prolonged interruptions.
- Assign responsibilities to designated personnel and provide guidance for recovery during prolonged periods of interruption.
- Ensure coordination with other personnel responsible for disaster recovery planning strategies. Ensure coordination with external points of contact and vendors and the execution of this plan.
- Provide ongoing updates to the Customer in line with any agreed specific escalation process and provide a post-incident report within 48 hours of the services being resumed, outlining all steps undertaken during invocation.

8.6 Plan Testing

The SaaS Disaster Recovery Plan is tested, as a live exercise or a table-top test, every six months. The tests are used for training operations personnel and are coordinated with all personnel responsible for contingency planning and execution. The tests verify that backups can be recovered and the procedures for shifting service to the alternate processing site are adequate and effective. Results of the testing are used to improve the process and initiate corrective actions.

9. PRIVACY

Encode takes steps to protect the privacy of our customers and protect data stored within the platform. Some protections inherent to Encode's product include authentication, access controls, data transport encryption, data at rest encryption, and HTTPS support. Where relevant, trusted keys and certificates are used, and appropriate management procedures are in place. Additional information can be found in our Privacy Policy.

10. ACCESS TO CUSTOMER DATA

Encode, or sub-contractor staff do not access or interact with Customer Data or applications as part of normal operations. There may be cases where Encode or a sub-contractor is requested to interact with Customer Data or applications at the request of the customer for support and consulting purposes or where required by law. Customer Data is access controlled, and all access by Encode or sub-contractor staff is accompanied by customer approval or government mandate, reason for access, actions taken by staff, and support start and end time. All access is based on least privilege, logged and is regularly reviewed and removed immediately when no longer required. All access is managed in conjunction with a customer employee.

11. CUSTOMER DEFINED DATA RETENTION

During an Encode SaaS active subscription term, the Customer has the freedom to define what data its Encode applications store and the ability to purge data from their databases and file systems to comply with their data retention requirements.

12. STORAGE CAPACITY

Where the Customer is likely to reach the agreed maximum storage capacity, Encode will promptly send a warning to the Customer in writing. The Customer must then within a reasonable time period either decide to reduce the stored data to keep the data within the agreed maximum storage capacity or purchase additional storage capacity, to be mutually agreed in good faith between the Parties. In the interim, the Supplier will support with additional and reasonable storage capacity to ensure that no Customer Data is lost. In the event that the Supplier fails to notify the Customer promptly (or at all), the Supplier will support with additional storage capacity to ensure that no Customer Data is lost until such time as a solution is agreed. This clause takes precedence over the storage capacity provisions of any clauses in the Customer's Encode SaaS Agreement.

13. RETURN OF CUSTOMER DATA

With a valid subscription, Customer can request copies of Customer Data upon reasonable written request at any time if the methods provided within the Encode SaaS application do not meet the Customer's requirements. Encode will provide a cost estimate to the Customer for approval before execution and data delivery.

Encode will in good time, upon notification of contract termination or expiry, assist the Customer in performing a termination review, identifying all data to be extracted, packaged and returned and execute the return of all data at no additional charge or delete where the return is not possible.

Encode shall provide such Customer Data requests via a downloadable file in comma-separated value (.csv) format and attachments in their native format. Encode shall provide the downloadable file either via a secure HTTPS

download link, SFTP server or another method that shall be mutually agreed with the Customer.

14. DELETION OF CUSTOMER DATA AFTER TERMINATION

After termination or expiry of all subscriptions associated with an environment, Customer Data submitted to the Encode SaaS is securely overwritten or deleted from production, sandboxes and backups within 1 working day of the termination date.

15. STAFF SCREENING, SECURITY TRAINING AND AWARENESS

15.1 Screening

As a condition of employment, all Encode employees undergo pre-employment background checks and agree to company policies, including security and acceptable use policies.

15.2 Training

All employees have security responsibilities detailed within their job descriptions and terms and conditions of employment, and regular security training is undertaken throughout their employment.

15.3 Security Staff

Our information security team is responsible for application and information security. The security team works closely with the entire Encode organisation and customers to address risk and continue Encode's commitment to trust.

16. USAGE ANALYTICS

Encode may track and analyse the usage of Encode SaaS for purposes of security and for helping Encode improve both the Services and the user experience in using the Services. For example, Encode may use such information to understand and analyse trends or track which of the features are used most often to improve product functionality. Encode may share anonymous usage data with Encode's service providers for the purpose of helping Encode in such tracking, analysis and improvements. Additionally, Encode may share such anonymous usage data on an aggregate basis in the normal course of operating our business; for example, we may share information publicly to show trends about the general use of our services.