Technical and organisational security measures for protection of sensitive data in CSC Sensitive Data services

This document describes the primary security design for CSC's Sensitive Data services. CSC is a reliable partner whose data centres have been granted an ISO/IEC 27001 certificate for their information security management systems. These information security management systems ensure that the CSC possesses the capacity to manage, govern and continuously develop the information security of its services and operations. Please, see https://www.csc.fi/security for more information on our security, which is also the basis for our Sensitive Data (hereafter, SD for short) services.

The following sections define the current additional technical and organisational measures, on top of the standard CSC security measures, on CSC's Sensitive Data services, consisting of SD Apply, SD Connect, SD Desktop, SD Submit, and Federated EGA, and are part of Data Processing Agreement (DPA). CSC may change these at any time without a notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

1. DATA PROTECTION OFFICER

CSC has an appointed Data protection officer, see https://www.csc.fi/en/privacy for more information and contact details.

2. DATA PSEUDONYMISATION

The Services do not include a pseudonymisation service for User Content. This means that the user will have the sole responsibility for the legality and security measures of processed User Content.

3. DATA TRANSPORT SECURITY

All external data transport with the Services is secured by Transport Layer Security (TLS) version 1.2 or later. This means that all user interactions with the Services, including transfer of User Content, are using HTTPS over TLS communication and hence, use strong encryption for the transport.

Sensitive User Content is encrypted with a strong encryption algorithm prior to transport at user's end. This means that, prior to transport of User Content, the tools provided by the Services encrypt the User Content automatically.

Any User Content in SD Desktop cannot be transported out from the Service by the user. This means that the user must request, in written, that she/he wishes to copy Use Content out from

the Service. The user requesting the data transport has to be the project manager of the registered CSC project in question, and the request must contain information about which data is to be copied, and provide an adequate location for storing the copy of the data. The requested data must be encrypted before copying.

All internal data transport within the Services is secured by Transport Layer Security (TLS) version 1.2 or later, where applicable. This means that all communication within the Services — internal communication between service components — are using HTTPS over TLS communication and hence, use strong encryption for the communication channel.

There are perimeter firewalls, edge routers and, where applicable, secure gateways to block unused protocols and services. This means that traffic from outside, and between, of the Services, is limited to the minimum required in order to provide the Services for the user.

Internal firewalls, routers, access control lists (ACLs), and network segments segregate traffic between the application, storage, database, and management tiers. This means that various service components of the Services are segmented into different networks, which have network access policies in place to limit the allowed traffic to the absolute minimum required for the service components to work.

4. DATA STORAGE SECURITY

Sensitive User Content is encrypted with a strong encryption algorithm prior to storing, and is stored at CSC's data centres in Finland. User may opt to store sensitive User Content unencrypted in hers/his SD Desktop. This means that by default all User Content is encrypted while stored, but for certain purposes, e.g. to speed up analysis, the user may choose to store some User Content unencrypted in their own private computing environment.

Non-sensitive information may be stored encrypted or unencrypted, depending on customers' preferences, at CSC's data centres in Finland. This means that the user may opt out on using encryption for non-sensitive data, such as tools, scripts, or analysis pipelines, but sensitive data must still always be encrypted according to Service Descriptions.

The Federated EGA Service may store non-sensitive information outside CSC's data centres. This means that, due to the nature of the Service, certain metadata describing the sensitive User Content and its usage are stored at Central EGA and/or at other participating nodes in the federation. This includes personal data, such as user IDs, IP addresses, and other such information the user has granted the Service access to.

SD Submit and Federated EGA Services maintain a secondary copy of User Content. This means that those mentioned Services keep a backup copy of User Content, stored at a secondary location, but no other Service maintains such a copy.

Data needed for providing the Services, such as configurations, logs, and encryption keys, are protected with various methods, such as access control lists (ACLs), segmentation, and

encryption. This means that all the data the Services need to operate, and the data they generate, have either restricted or controlled access, and are distributed and administered by different tiers.

5. DATA COMPUTING SECURITY

The computing environment where the User Content is being processed is an isolated processing environment. This means that the computing environment is isolated from the Internet and all other networks with gateways, firewalls, routers, network segmentation, and access control lists (ACLs). Furthermore, each registered CSC project is isolated from each other with the same techniques.

The SD Desktop is protected with a data diode. This means that, apart from the screen image of the isolated compute system, no data can be taken out from the Service except as described in the Data storage section.

6. DATA ACCESS SECURITY

User management and access to Services and hence, to User Content, is controlled by CSC account and project management process, see https://docs.csc.fi/accounts/. This means that all users having a membership in the same project may have access to User Content, and that the project manager is responsible for maintaining the project's membership.

For SD Apply and Federated EGA the access to User Content is controlled by data access grants. This means that only those users who have been granted access to User Content are able to access it. No other users, even in the same project, can access such data access grant controlled User Content. The access is granted by a data access committee set by the User Content owner.

User interactions with the Services are logged. This means that user actions regarding logging in to and out from the Services, and any transfers of User Content are recorded.

Actions regarding processing of User Content in the SD Desktop are not logged. This means that user actions regarding viewing, analysing, or copying the data inside the Service are not recorded.

Administrative access to the Services is controlled by CSC administration guidelines, and is limited to select CSC administrators only. There is a separation of duties, e.g. service administration, network administration, and storage administration.

7. ADDITIONAL SECURITY MEASURES

The Services are being monitored for any issues or unusual behaviour. This means that we are actively monitoring the Services for access, network and storage usage, and other measures, in

order to ensure availability and security of the Services, and to detect any unwanted or otherwise suspicious activity.

The Services are being regularly scanned for vulnerabilities and other weaknesses. This means that CSC internal security team will scan the Services regularly in order to verify no unspecified network services or ports are available, and that no known vulnerabilities exist on the Services.

Security patches are being applied regularly. This means that we keep our software up to date, and apply patches regularly on all systems needed for the Services. Critical security patches are applied as soon as possible.

The personnel managing, administering, and developing the Services are being regularly trained for sensitive data processing according to general CSC training processes. This means that additional training, such as CIPP/E, are being applied for the personnel responsible for the Services.