Este documento descreve os requisitos a serem cumpridos por terceiros (parceiros, fornecedores, subcontratados, etc.), doravante referidos como «Parte Receptora», relativamente ao tratamento de informação sensível da EID.

As informações sensíveis incluem toda a informação classificada como:
- «EID RESTRICTED»
- «EID CONFIDENTIAL»
- «EID SECRET»

Caso a Parte Receptora receba quaisquer informações da EID e não tenha a certeza de como lidar com essas informações deve contactar o CISO (Responsável pela Segurança da Informação) da EID para obter instruções.

REQUISITOS

1) Confidencialidade e partilha

As informações devem ser mantidas em sigilo absoluto e só podem ser divulgadas aos funcionários da Parte Receptora com base na «necessidade de saber» (ou seja, o acesso só deve ser concedido se as informações forem estritamente necessárias para o cargo e o trabalho a ser realizado para os fins para os quais as informações foram fornecidas). A partilha com outras partes externas (outras entidades jurídicas, incluindo entidades afiliadas) só é permitida após a aprovação da EID.

O acesso e a distribuição de informação classificada como «EID SECRET» devem ser registados (data, hora, remetente, destinatário, finalidade). Estes registos devem ser facultados para consulta se solicitado pela EID.

2) Divulgação não autorizada

Em caso de divulgação não autorizada de informação sensível, a Parte Receptora deve comunicar imediatamente tal evento ao CISO da EID.

3) Informações físicas

Deve-se tomar cuidado ao imprimir e copiar informação sensível (limitar sempre ao absolutamente necessário).

A informação sensível deve ser triturada e descartada de forma segura.

A informação física «EID CONFIDENTIAL» e «EID SECRET» deve ser arquivada num local de armazenamento trancado e/ou numa área de acesso controlado (acesso de acordo com o princípio da necessidade de saber). A informação «EID SECRET» deve ser transportada em envelope selado e apenas entregue em mão.

4) Requisitos de armazenamento e acesso a dados digitais

	ARMAZENAMENTO EM CLOUD	**ARMAZENAMENTO LOCAL**	**ARMAZENAMENTO EM SUPORTES PORTÁTEIS (EX: PEN USB)**
Accesso	Limitado de acordo com o princípio da necessidade de saber		
	Protegido com autenticação multifatorial	• Protegido com autenticação multifatorial • Acesso sem autenticação multifatorial, áreas com controlo de acesso na rede da empresa	N/A
	Necessária monitorização (quem tem acesso a quais dados e quando)		N/A
	Limitado a terminais definidos	Acesso externo é limitado aos terminais definidos	N/A
Utilizadores	As identidades dos utilizadores são rastreáveis a pessoas singulares		N/A
Encriptação	Os dados arquivados e em trânsito são encriptados (pelo menos nível AES256)		Dados são encriptados (pelo menos nível AES256)
Localização	Os dados são armazenados no Espaço Económico Europeu (EEE)	N/A	N/A

N/A: Não Aplicável

Os requisitos acima mencionados também se aplicam a cópias de segurança que possam incluir informação sensível.

5) Eliminação de dados digitais

A informação sensível que deixe de ser necessária deve ser eliminada permanentemente da rede ou do dispositivo (não removidas para a reciclagem).

6) Exceções a esta Política de Segurança

As exceções aos requisitos desta política só são permitidas após aprovação explícita por escrito do CISO da EID.

Contactos

Ricardo Costa
CISO (Responsável pela Segurança da Informação)
Telefone 212 948 600
Email: ricardo.costa@eid.pt

This document describes the requirements to be met by third parties (partners, suppliers, subcontractors, etc), hereinafter referred to as "Receiving Party", regarding the handling of EID's sensitive information.

Sensitive information includes the information classified as:

- «EID RESTRICTED»
- «EID CONFIDENTIAL»
- «EID SECRET»

In case the Receiving Party receives any EID information and it is unclear how to handle such information, the Receiving Party should contact EID's CISO (Chief Information Security Officer) for instructions.

REQUIREMENTS

1) Confidentiality and Sharing

Information must be kept in strict confidence and may only be disclosed to the employees of the Receiving Party on a "need to know" basis (i.e. the access should only be granted if the information is strictly required for the position and work to be performed for the purpose to which the information has been provided). Sharing with other external parties (other legal entities, including affiliated entities) is only allowed after EID's approval.

Access to and distribution of information classified as "EID SECRET" must be registered (date, time, sender, recipient, purpose). An overview of the register(s) must be provided, if requested by EID.

2) Unauthorized Disclosure

In case of any unauthorized disclosure of sensitive information, the Receiving Party must immediately report such event to EID's CISO.

3) Physical Information

Caution should be used when printing and copying sensitive information (which should always be limited to the absolutely necessary).

Sensitive information must be shredded and securely disposed of.

Physical "EID CONFIDENTIAL" and "EID SECRET" information must be stored in a locked storage mean and/or in an access-controlled area (access according to the need-to-know principle). "EID SECRET" Information must be transported in a sealed envelope and delivered only in hand.

4) Digital Data Storage and Access Requirements

	CLOUD STORAGE	ON PREMISES STORAGE	PORTABLE DATA CARRIERS (E.G., USB STICKS)
Access	Limited according to the need-to-know principle		
	Secured with multi-factor authentication	• Secured with multi-factor authentication or • Access without multi-factor authentication only on company network in access-controlled areas	N/A
	Monitoring required (who has access to which data and when)		N/A
	Limited to defined endpoints	External access is limited to defined endpoints	N/A
Users	User identities are traceable to natural persons		N/A
Encryption	Data at rest and in transit is encrypted (at least level AES256)		Data is encrypted (at least level AES256)
Location	Data is stored within the European Economic Area (EEA)	N/A	N/A

N/A: Not Applicable

Above-mentioned requirements are also applicable to backups on which sensitive information is stored.

5) Deletion of Digital Data

No longer needed sensitive information must be permanently deleted from network or device (not removed to recycle bin).

6) Exceptions to this Security Policy

Exceptions to requirements in this policy are only allowed after explicit written approval from EID's CISO.

Contact Details

Ricardo Costa
(CISO) Chief Information Security Officer
Telephone: 212 948 600
Email: ricardo.costa@eid.pt