EUROPEAN
COMMISSION

Brussels, 4.11.2019
C(2019) 8016 final

IT security standard

Backup

CONTENTS

1. INTRODUCTION

In accordance with Commission Decision (EU, Euratom) 2017/46 and Commission Decision laying down the implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission, C(2017)8841, and in particular Article 12, the standard on backups relating to Commission Decision C(2006) 3602 should be repealed.

Backups of data stored electronically are a cornerstone of information security, providing the possibility of recovery from a very wide range of risks. Backing up data helps to protect it against breaches of availability and integrity. Backups are an essential component of any disaster recovery plan supporting business continuity.

Nevertheless, backups are useless if they cannot be restored, so testing and restoration procedures are as important as the procedures for making backups.

2. PURPOSE

This standard provides the appropriate controls to follow to back up all types of electronically stored data on IT systems, including servers and network equipment.

The goal of this standard is not to force all data to be backed up but to ensure that system/data owners identify the data that require backing up and implement backup procedures accordingly. The frequency and type of backups should be based on an analysis of the availability and integrity requirements of the data (e.g. during the analysis phase of the business continuity planning process). Based on this analysis, the system owner should decide which of the backup plans offered in the service catalogue of the IT service provider is suitable for their IT systems.

3. SCOPE

This document sets out the minimum requirements that apply to all applications and IT systems hosted on European Commission premises. Some are mandatory and subject to compliance verification. Some are in the form of recommendations (i.e. guidance) based on industry best practices, and not subject to compliance verification. These may become mandatory in future versions of this standard, in the light of customer feedback, further best practices identified and compliance analysis.

The archiving of data falls outside the scope of this standard. Workstations and mobile devices are also outside its scope.

4. EXCEPTIONS

This security standard is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision laying down the implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission, C(2017)8841.

5. DEFINITIONS

For the purposes of this standard, in addition to the definitions provided in Article 2 of Commission Decision (EU, Euratom) 2017/46 and Article 2 of Commission Decision laying down the implementing rules for Articles 3, 5, 7, 8, 9, 10, 11, 12, 14, 15 of Decision 2017/46 on the security of communication and information systems in the Commission, C(2017)8841, the following definitions also apply:

TERM	DEFINITION
application business data	Information that is used to plan and run a business. This includes source data that a business collects and data that has been processed. This means business data held in applications and databases that are machine-readable or represented as information intended for human consumption such as a user interface, document or report.
backup	The process of copying data to a separate store in order to protect it from unavailability or corruption of the principal store; also the data so stored.
configuration	Configuration data for operating systems, application systems, network devices etc that changes occasionally.
data store	Repository for consistently storing and managing collections of data which include not just repositories like databases, but also simpler store types such as simple files, emails, etc.
full backup	A backup consisting of a complete, new copy of all data of an IT system.
journal (file)	Complete record of all database modifications (when enabled) at the level of the data. If some modifications are lost, for example because they occurred after the most recent backup of a recovered database, they can be restored to the database by replaying the journal file.
programs	Operating system, middleware, application code (compiled or not) and application system files that rarely change (i.e. executable and other files that are installed as part of the system).
recovery point objective (RPO)	The maximum permissible data loss interval defined for business continuity purposes. The interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the business continuity plan's maximum allowable threshold or "tolerance."
recovery time objective (RTO)	The period defined for business continuity purposes within which a system and its data must be recovered.
restoration	The process of copying data back to the principal store (or an alternative) from the backup store.
test data (development/test systems)	Application/Business data used for testing and development.

6. GENERAL REQUIREMENTS

(M=mandatory, R=recommended)

S/N	Requirement	Implementation
1.	Backups of application business data on production systems **shall** be taken to ensure that all necessary data can be recovered.	M
2.	A system backup, including programs and configuration of at least one previously reliable instance or image **shall** be retained as a fall-back in case of problems before changes.	M
3.	Test data **should** be backed up. The decision for backing it up and the frequency of the backups should be determined through the risk assessment or testing requirements.	R
4.	Measures such as journaling **should** also be considered for application business data.	R
5.	For the IT systems hosted in the infrastructure and the data of the applications, IT service providers **shall** document their backup policy into the service catalogue.	M

7. BACKUP

To maintain the integrity and availability of data and data processing facilities, backups of data and software shall be made in accordance with established procedures. They shall be regularly tested, including the timely restoration of data.

7.1. General rules

(M=mandatory, R=recommended)

S/N	Requirement	Implementation
6.	If a backup media in transit is the sole copy of the data (e.g. a backup being transported to a different location for restoration when the primary copy has been destroyed), it **shall** be highly[1] protected for availability reasons.	M
7.	Data contained in backups **shall** be protected to at least the same level as the data in the operational systems, and higher if necessary. The evaluation **shall** be based on a risk assessment including the backup process itself, risk of data aggregation on storage media, risk to data-in-transit or risk to data stored in online backup systems.	M
8.	Security measures **shall** be taken to protect backups of sensitive non-classified information against unauthorised access during	M

[1] More information on restoration and protection is provided in the business continuity management standard.

S/N	Requirement	Implementation
	transmission, storage and physical transportation. The use of encryption[2] is recommended, taking into account the risks and other countermeasures in place.	
9.	Backup mechanisms **shall** be automated to ensure that they are performed consistently and according to the backup objectives and RTO/RPO defined for business continuity purposes.	M
10.	A complete record of available backups and media **shall** be maintained (and duplicated at a remote site in case of loss of the primary record), including the following information for each backup: • date and time of backup; • backup content, i.e. directory names or other documented reference; • identification of the location of the original data store; • identification of the media on which the backup data is stored; • identification of the hardware and software used for taking the backup; • other information concerning the type of backup (daily backup of data, etc.); • reference to the procedure required for information restoration. Appropriate security controls **shall** be implemented to safeguard the confidentiality of this record. The controls must be based on a risk assessment.	M
11.	A check **shall** be performed on the existence and presence of all media at least once per year, to ensure that none have been lost or stolen.	M
12.	Backup media **shall** be replaced in a cycle based on the manufacturers' recommendations for the usable lifetime of the media, or earlier if found to be defective.	M
13.	Media used for backups **shall** be handled with care, and obsolete backup media **shall** be disposed of securely[3].	M
14.	Only authorised staff **shall** have access to the backup store(s).	M
15.	In the event of any conflict between backup requirements (generally for availability purposes) and data protection	M

[2] Encryption shall comply with the standard on cryptography and public key infrastructure.
[3] For more details refer to the standard on sanitisation of media.

S/N	Requirement	Implementation
	requirements, advice **shall** be sought from the Data Protection Officer, and the resulting decision should be documented.	

7.2. Testing and Restoration

(M=mandatory, R=recommended)

S/N	Requirement	Implementation
16.	Backup media **shall** be regularly tested (at least once per year) to ensure that they can be relied upon for use when necessary.	M
17.	Restoration tests **shall** be conducted when the backup configuration, procedure or technology is changed.	M
18.	More extensive restoration tests **shall** be conducted in line with business continuity testing requirements[4]. System owners are responsible for initiating these tests.	M
19.	The test procedure **shall** prove at least that: • complete data and system restoration is possible; • the data can be installed on an alternative system; • the staff involved are fully aware of the procedures required to take backup copies and to restore the data.	M
20.	Unsuccessful tests **shall** be investigated to identify and correct any problems, and the test must be repeated until it succeeds.	M
21.	Restoration tests **shall** be performed on the last backup.	M
22.	Data restorations **shall** be properly authorised.	M
23.	Data **shall** only be restored to the original location or another pre-determined and authorised location.	M

8. Roles and Responsibilities

(M=mandatory, R=recommended)

S/N	Requirement	Implementation
24.	The system/data owner **shall** define the RPO and RTO for business continuity purposes.	M

[4] Critical systems should undergo full backup tests every year, in line with business continuity testing requirements.

S/N	Requirement	Implementation
25.	The system/data owner **shall** approve backup arrangements.	M
26.	The system/data owner **shall** ensure that backups are performed and tested in line with the aforementioned rules.	M
27.	The system/data owner **shall** ensure that backups are held and transported securely, in line with the requirements of this standard.	M
28.	The system/data owner **shall** ensure that the backup needs of their IT systems are met by the backup services offered by IT service providers.	M
29.	The data owner **shall** approve data restores as a request for service.	M
30.	The data owner **shall** confirm that all data has been properly restored at the end of the process.	M
31.	IT service providers **shall**: • operate the backup and restoration solution; • schedule backups according to the system/data owner's requirements; • verify the effectiveness and reliability of the backup solutions (e.g. by testing the backups); • restore backups upon receipt of a properly authorised request, or make controlled mechanisms available for system owners to perform such restorations; • maintain an inventory of backup media and their contents; • inform the system/data owner about the default backup level of their IT systems; • promptly notify the system/data owner about the success or failure of the backup of their IT systems; • securely erase a backup on request of the system owner. • refer in the service catalogue the backup and restoration service-level agreements for the generic solutions they provide.	M

9. ENTRY INTO FORCE

This standard shall enter into force on the day following the date of adoption of this standard.