EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate DS - Security
Coordination and Informatics Security

Brussels, 17/02/2011
HR.DS5/GV/ac ARES (2011) 176475
SEC20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

STANDARD ON BACK-UPS

ADOPTED BY MRS. IRENE SOUKA,

DIRECTOR-GENERAL OF DG HUMAN RESOURCES AND SECURITY, ON 17/02/2011

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.

Commission européenne, L-2920 Luxembourg. Telephone: (352) 43 01-1.

TABLE OF CONTENTS

1. ADOPTION PROCEDURE 3
2. INTRODUCTION 3
3. OBJECTIVES 3
4. SCOPE 4
5. THREATS COVERED 4
6. TERMINOLOGY 5
7. BACKGROUND INFORMATION 5
8. BACK-UP 7
8.1. General rules 7
8.2. Personal Information 10
9. TEST AND RESTORE 10
9.1. Testing 10
9.2. Restore 11
10. ROLES AND RESPONSIBILITIES 11
11. REFERENCES 11
12. RELATED DOCUMENTS 12

1. ADOPTION PROCEDURE

This Security Standard is adopted in accordance with Article 10(3) of Commission Decision C(2006) 3602 concerning the security of information systems used by the European Commission, adopted on 16 August 2006.

It is drawn up under the responsibility of the Security Directorate pursuant to Article 9(1)(b) and takes into account the items listed in Article 10(2) of Commission Decision C(2006)3602, in particular internationally recognised norms and standards applicable in the field of information systems security.

Under Article 10(3) of Commission Decision C(2006) 3602, the implementing rules may be supplemented by measures of a technical, physical, procedural or organisational nature proposed by the Director of the Security Directorate and adopted by the Director-General of the Directorate-General for Human Resources and Security in consultation with departments that have a legitimate interest. These supplementary measures are called 'security standards' where their application is mandatory, or 'security guidelines' where their application is optional or where they provide guidance on security standards implementation.

2. INTRODUCTION

Back-ups of data stored electronically are a cornerstone of information security, providing the possibility of recovery from a very wide range of risks, both known and unknown. Backing up information helps to protect it against breaches of availability and integrity, and is useful in protecting against almost all such threats. Back-ups are an essential component of any business continuity plan.

Performing effective back-ups is, however, neither simple nor cheap. The massive growth in the quantities of data stored at the Commission means that back-up facilities need to develop just as quickly in order to maintain the level of protection provided. The technologies and processes involved must therefore be managed with great care.

Back-ups are useless if they cannot be restored, so testing and restoration procedures are as important as the procedures for taking back-ups.

This standard provides rules on defining and applying back-up controls to all kinds of information, with the goal of ensuring that the relevant procedures are optimised to protect information whilst neither jeopardising recovery times nor incurring excessive costs.

3. OBJECTIVES

This standard provides instructions for the procedures to be used for backing up all types of electronically stored information on all types of computer systems, including servers, network equipment, workstations, mobile devices and data storage media.

4. SCOPE

This standard applies to all data that is stored electronically by the Commission on all devices, including but not limited to the following: servers, workstations, portable PCs, other portable computing devices (PDAs etc.), storage devices, network equipment and media storage (floppy disks, USB devices etc.). The measures mandated by this standard must be followed by all relevant personnel, including all Commission officials, contractors and third parties in possession of such information.

This standard applies to both EUCI and non-EUCI. Additional measures may be required for EUCI (see Commission Decision (2001/844/EC, ECSC, Euratom) of 29/11/2001).

Archiving of information is outside the scope of this standard.

5. THREATS COVERED

Security controls defined in this security standard will help to reduce the impact of the following threats (their description is in the Standard on Information Security Risk Management). Back-ups are a very important control and help to remediate almost all threats potentially impacting availability and integrity.

T01 – Fire

T02 – Water damage

T03 – Pollution

T04 – Major accident

T05 – Destruction of equipment or media

T06 – Climatic phenomenon

T07 – Seismic phenomenon

T08 – Volcanic phenomenon

T09 – Meteorological phenomenon

T10 – Flood

T11 – Failure of air-conditioning

T12 – Loss of power supply

T13 – Failure of telecommunication equipment

T14 – Electromagnetic radiation

T15 – Thermal radiation

T16 – Electromagnetic pulses

T21 – Theft of equipment

T24 – Data from untrustworthy sources

T26 – Tampering with software

T28 – Equipment failure

T29 – Equipment malfunction

T31 – Software malfunction

T36 – Corruption of data

T38 – Error in use

T39 – Abuse of rights

T40 – Forging of rights

6. TERMINOLOGY

Archiving: The process of moving information that is no longer regularly used to other storage media (often off-line, less expensive and/or more durable) for long-term retention.

Back-up: 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.

Full back-up: A back-up consisting of a full, new copy of all data. See also "Incremental Back-up".

Incremental back-up: A back-up consisting only of files or data that have been modified since the last back-up. This type of back-up is typically much faster to take, but must be restored in conjunction with the last (full) back-up, complicating and slowing the restore process. One common back-up strategy is to take a full back-up each weekend and an incremental back-up every night during the working week.

NAS: Network Attached Storage – a common term for storage devices with a file system connected to a network. NAS devices are often used for back-ups.

Recovery Point Objective (RPO): The maximum permissible data loss interval defined for Business Continuity purposes (often one day). This helps to determine the required frequency of data back-ups. The possible values defined in the *Standard on Business Continuity Management* are: 1 day or more; around ½ day or more; a few hours but < ½ day; a few minutes; or no loss at all.

Recovery Time Objective (RTO): The period defined for Business Continuity purposes within which a system and its data must be recovered. This is a critical factor in determining the technology to be used for taking and restoring back-ups. The possible values defined in the *Standard on Business Continuity Management* are: several months; 1 or 2 weeks and above; 1 or 2 days; hours but less than a day; or almost immediately (seconds or minutes).

Restore: The process of copying data back to the principal store (or an alternative) from the Back-up store.

7. BACKGROUND INFORMATION

Information is held electronically in many different places at the Commission. Some of this information is centrally controlled, such as information in formal

information systems, and is likely to be well protected. Other information is held on end user devices, and is not so well controlled.

Back-ups are a major component of business continuity planning, and this standard should be read together with the *Standard on Business Continuity Management*.

The goal of this Standard is not to force all data to be backed up, but to ensure that data that should be backed up is identified and then treated as appropriate. The frequency and type of back-ups taken should be based upon an analysis of the availability and integrity requirements of the information[1] (e.g. during the analysis phase of the business continuity planning process).

The following table is intended to help clarify the different types of data that may exist.

Data Type	**General Comments**	**Back-up Comments**
PROGRAMS	Operating system and application system files that changes rarely (i.e. executable and other files that are installed as part of the system)	Should be backed up at infrequent periods and after changes. A back-up of at least one previously known good configuration must also be retained as a fallback in case of problems.
CONFIGURATION	Configuration data for operating systems, application systems, network devices etc that changes occasionally	Must be backed up periodically and after changes. A back-up of at least one previously known good configuration must also be retained as a fallback in case of problems.
LOGFILES	Event logs from operating systems, network devices, applications etc.	May or may not require back-up; should be determined through analysis of requirements.
APPLICATION DATA (Production systems)	Data held in application systems, either directly or by other data storage systems used by the application.	Must be backed up frequently (often daily). Other measures such as journaling may also be required.

[1] Note that the normal data classifications defined in the Commission Decision C(2006) 3602 (PUBLIC, LIMITED etc) cannot be used to determine back-up requirements, since this classification is based on the confidentiality of the information. The levels of integrity and availability that are defined in C(2006) 3602 – MODERATE, CRITICAL and STRATEGIC – may be of help, but are still not directly linked to the time criticality of the application.

Data Type	General Comments	Back-up Comments
TEST DATA (Development/Test Systems)	Application data used for testing and development.	Back-ups are facultative rather than mandatory. Frequency should be determined according to the work involved in recreating the data. If data is a simple copy of production data, no back-up may be necessary; if considerable work has gone into creating a test data set, then it is advisable to back it up periodically.
PROGRAM CODE	Programs under development (i.e. the program code, as distinct from the test data in the previous example).	Must be backed up frequently, e.g. daily incremental and weekly full back-ups.
USER DATA	Files that are created and/or used directly by users, such as Office documents. These files may be stored on file servers or on user devices (workstations, PDAs etc.). Personal data is also commonly stored on EC equipment, for which there is no business need to back up.	Files that are stored on file servers must be backed up frequently, e.g. daily incremental and weekly full back-ups. For files stored on user devices, back-ups are not mandatory; users should be informed whether files are backed up and advised on where to store files that need to be backed up.
ELECTRONIC MAIL	Email data is generally held in an application data store of some kind, and is often archived automatically. It requires specific attention due to the often underestimated criticality of email systems.	Back-ups must be at least daily.

8. BACK-UP

Policy objective 5.5.1 – Back-up – To maintain the integrity and availability of information and information processing facilities, Back-ups of information and software must be made in accordance with established procedures. They must be regularly tested, including the timely restoration of information.

8.1. General rules

Back-ups of information in production systems must be taken to ensure that all essential information and software can be recovered when required. Back-ups protect the availability and integrity of information; however, since

back-ups often consist of a great deal of data stored in one place, they also represent a risk to information confidentiality.

A detailed back-up policy must be documented for each information system which must specify the following elements[2]:

- The information to be backed up must be clearly defined. This must include all operating system and configuration files, application files and data.

- The frequency of back-ups. They may be different for different types of data (see table in section 6 above for further information), and should be based on the information system's RPO, where defined.

- The required time for the restoration of the back-ups, based on the information system's RTO, where defined.

- The type (e.g. full, incremental or differential[3]) of back-ups. A combination of different back-up types may be used. This combination should be determined in order to maximise the efficiency of the back-up operations whilst ensuring timely restoration (as per the previous point).

- The number (and type, if relevant) of back-up generations to be retained (a very simple example may be all incremental or differential back-ups since the last full back-up, and the last 4 full back-ups).

- The location where the back-ups are stored. At least one recent back-up should be stored at a remote location, at a sufficient distance to escape any reasonable damage at the main site (this should be determined by the Business Continuity process). Remote mirrored systems must not be used as the only back-up for critical data since software problems can affect both systems and render data unusable.

- The Recovery Time Objective of the information being backed up. This RTO must enable recovery of the original data within the maximum unavailability period (as defined in the IT Security Plan), in case of integrity or availability failure. This RTO must be determined in compliance with business continuity management.

- The frequency for testing restoration procedures (see section 9 below).

- The back-up retention/erasure period.

---

[2] If a standard back-up service is used which fulfils the system's back-up requirements, the back-up policy may simply refer to the documentation of that service.

[3] There are a number of different types of back-up depending on the technologies used. The terms "Full", "Incremental" and "Differential" are the most commonly used, but their inclusion here does not exclude the use of other back-up types.

- Security requirements for back-up stores, including:
    - Security measures during transportation of back-up media
    - Measures to protect media against unauthorised access (e.g. for making illicit copies)
- The responsibilities for back-up.

Back-up facilities must be automated to ensure that they are performed regularly and consistently. A complete record of the available back-ups and media must be maintained (and duplicated at a remote site in case of the loss of the primary record), including the following information for each Back-up:

- Date of back-up;
- Back-up content, i.e. directory names or other documented reference;
- Identification of the location of the original data store (production environment);
- Identification of the media on which back-up information is stored;
- Identification of the hardware and software used for taking the back-up;
- Other information concerning the type of the back-up (daily back-up of information, etc.);
- Reference to the procedure required for information restoration.

An inventory of all back-up media must be maintained that enables cross-checking the media to ensure that none have been lost or stolen. A check (automated or manual) must be performed at least once a year.

Back-up media must be replaced in a cycle based on the manufacturers' recommendations for the usable lifetime of the media, or earlier if found to be defective. Media used for back-ups must be handled with care, and obsolete back-up media must be disposed of securely (see the *Standard on Sanitisation of Media*).

Information contained in back-ups must be protected to at least the same level as the information in the operational systems, and higher if necessary to counter the effect of data aggregation since back-up stores contain large volumes of data. Only authorised staff is permitted to have access to the back-up store(s).

The security of back-up media in transit must be considered, particularly concerning threats to data confidentiality. In the event that a back-up in transit is the sole copy of that information (e.g. a back-up being transported

to a different location for restoration when the primary copy has been destroyed), it must also be highly protected for availability reasons.

As technology is always developing and new solutions may become available, other back-up architectures than those envisaged here may be used as long as the principles in this standard are applied.

8.2. Personal Information

Back-ups of personal information must comply with the Commission's Data Protection requirements. In the event of any apparent conflict between the back-up requirements (generally for availability purposes) and the data protection requirements (for confidentiality), advice may be sought from the EDPS and the Security Directorate and the resulting decision documented.

9. TEST AND RESTORE

Policy objective 5.5.1 – Back-up – To maintain the integrity and availability of information and information processing facilities, Back-ups of information and software must be made in accordance with established procedures. They must be regularly tested, including the timely restoration of information.

9.1. Testing

Back-up media must be regularly tested to ensure that they can be relied upon for use when necessary. Partial tests (e.g. restoration of a small number of files picked at random) must be performed at least once a month, and more extensive tests at least once every two years (this may be performed during a business continuity exercise)[4].

The test procedure must prove at least that:

- The complete data restoration is possible;
- The restoration procedure meets the RTO defined by the system owner (i.e. the procedure can be performed within the required time).
- Information can be installed on an alternative system;
- The personnel involved are fully aware of the procedures required to take back-up copies and to restore the information,

The results of tests must be documented in a log. Unsuccessful tests must be investigated to identify and correct the problem, and the test repeated until it succeeds.

---

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

Where information must be kept for reasons other than facing IT contingency (e.g. for legal reasons), it should be stored in an archiving system. Where information is required to be held for long periods (many years or even indefinitely), the media must be tested regularly to ensure that the information can still be retrieved, and the information copied onto new media if required (e.g. due to media deterioration or technology changes). Suitable hardware must also be available to read the information.

9.2. Restore

Restoration procedures must be regularly checked and tested to ensure that they are effective and compliant with the RTO, i.e. that the restore can be completed in the required timescale. These tests should be performed on a recent back-up.

Care must be taken to ensure that data restorations are properly authorised. By default, data must only be restored to the original location or another pre-determined and authorised location. This rule may be bypassed in exceptional circumstances (e.g. during a major business continuity incident) with the approval of the System Owner.

10. ROLES AND RESPONSIBILITIES

System/Data Owner: responsible for defining the RPO and RTO, approving Back-up arrangements and ensuring that back-ups are performed correctly. Data owner is responsible for requesting data restores.

IT Service Providers (e.g. DIGIT): responsible for:

- Operating the back-up & restore solution.
- Scheduling back-ups according to the System Owner's requirements
- Verifying the effectiveness of the solution (e.g. by testing back-ups)
- Restoring back-ups upon receipt of a properly authorised request
- Maintaining an inventory of back-up media and their contents

LISO: Responsible for ensuring that back-ups are held and transported securely, in line with the requirements of the information thereon.

End Users: responsible for ensuring that important office documents and any other business-related electronic data are saved in a location (on the network or on workstations) where they will be backed up.

11. REFERENCES

Commission Decision C(2006) 3602 of 16/8/2006

Implementing rules for Commission Decision C(2006) 3602 of 16.8.2006.

Commission Decision (2001/844/EC, ECSC, Euratom) of 29/11/2001

Standard on Risk Management

Standard on Business Continuity Management

Standard on Sanitisation of Media

12. RELATED DOCUMENTS

International standard ISO/IEC 27001 – Second edition 2005-06-15

International standard ISO/IEC 17799 – Second edition 2005-06-15