Publications Office

Information Security Management

Publications Office Minimum Security Requirements

Type	Minimum Security Requirements	Status	Final
Version	3.1.1	Date	19/10/2017
Reference	MSM	Language	EN

References

Version	Name
3.0.0	Information Security Policy Statement
3.0.0	Baseline Information Security Policies (BISP)

Revision history

Version	Name
1.0.0	Initial release
3.1.1	Review

Table of contents

1. INTRODUCTION 3

1.1. Objectives and positioning 3

1.2. Information classification 4

1.3. Responsibility for security requirements 5

2. APPLICATION-LEVEL SECURITY 6

2.1. Identification, Authentication, Authorization 6

2.1.1 Web applications 6

2.1.2 Back-office applications 7

2.2. Input data validation 8

2.2.1 Web applications 8

2.2.2 Back-office applications 9

2.3. Control of internal processing 10

2.4. Error Handling 10

2.5. Cryptographic controls 10

2.6. Documentation and procedures 11

2.7. e-Commerce 11

2.8. Logging 12

2.9. Clock synchronization 12

3. SYSTEM-LEVEL SECURITY 13

3.1. System isolation 13

3.2. System configuration hardening 13

3.3. System utilities 13

3.4. Development, test and production systems 14

3.5. Security system acceptance tests 14

4. NETWORK-LEVEL SECURITY 15

5. PHYSICAL SECURITY 16

5.1. Access to the building by non-statutory staff 16

5.2. Within the building 16

5.3. Operations outside the building (outsourced) 16

6. EXPLOITATION-LEVEL SECURITY 17

6.1. Change Management 17

6.2. Business Continuity Management 17

7. THIRD PARTIES' OBLIGATIONS 18

7.1. Adherence to the BISP 18

7.2. Non-Disclosure Agreement 18

7.3. Third party access to Publications Office systems 18

7.4. Auditing & monitoring right 19

7.5. Obligation of reporting 19

7.6. Other obligations 19

1. INTRODUCTION

1.1. Objectives and positioning

The European Commission owns and maintains the overall EC Information Systems Security Policies (EC ISSP). The EC ISSP does not provide rules, procedures or guidelines for specific communication and information systems. It defines, however, the general framework[1] and implementing rules on the basis of which Directorate-General/Department's specific security policies and system specific security plans are derived. All such derived security policies and plans shall be consistent with the EC ISSP.

In line with this requirement, the Publications Office has developed its own specific Baseline Information System Security Policies (BISP).

The Publications Office BISP applies to information systems NOT processing EU CLASSIFIED information.

The BISP is a set of policies that define the boundaries within which all processes must take place. All products selected, processes, manuals and handbooks must be in compliance with the policy. The policy serves as main reference, to which all subsequent security documents, would it be Technical Security standards, User Security standards and Security procedures, must comply with.

The European Commission is committed to follow the COBIT framework to deliver IT governance to the business services. As part of this strategy, the Publications Office has been recommended by the EC auditor to implement the COBIT "Delivery & Support 5 – Ensure System Security" controls objectives.

To fulfil this requirement the Publications Office has adopted the ISO/IEC17799 standard *"Code of practice for Information Security Management" (ISO/IEC 27002)*. Considering the importance of Business Continuity at the Publications Office, the chapter 11 (Business Continuity Management) of the ISO/IEC 17799 has been supplemented with the British Continuity Institute (BCI) Publicly Available Standard (PAS) number 56 "*Good practice guide to Business Continuity Management*". Accordingly, the OP's BISP is structured in line with the 10 standard domains. The Business Continuity Management domain is replaced by the BCI PAS56 framework.

The present document defines the minimum security requirements in order to comply with the BISP Policies.

This set of minimum security requirements is attached to each *Call-for-Tender* issued by the Publications Office.

Information security controls must be considered at the systems and projects requirement specifications and design stage. Failure to do so can result in additional costs, less effective solutions, and in the worst case, inability to achieve adequate security. In order to assist the project owners to specify those security requirements, a simple check list of minimum security requirement is developed here under, based on common best practices and specialised organisation recommendations, such as OWASP, SANS, NSA and NIST.

[1] *(a) Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission.*
(b)Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.
(c) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.
(c) Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
(d) Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.
(e) Regulation (EU, Euratom) 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF).

1.2. Information classification

- **Confidentiality:** The Publications Office does not deal with EU CLASSIFIED information in the scope of its daily business, therefore the security requirements for EU CLASSIFIED information are out-of-scope of this document. In exceptional cases where it might be the case, classified information and data will be managed using specific security procedures based on the Commission decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.
  A realistic classification in terms of confidentiality must be defined by the system owner on the basis of the likely consequences that unauthorised disclosure might have for the interests of the Commission, the other Institutions, the Member States or other parties.

  The confidentiality levels for NON EU CLASSIFIED information are:

  - **PUBLIC**: information system or information intentionally prepared and compiled for public disclosure.
  - **LIMITED**: information system or information reserved for a limited number of persons on a need to know basis and whose disclosure to unauthorised persons might be prejudicial to the Commission, other Institutions, Member States or other parties, but not to an extent serious enough to merit classification as laid down in article 3 of the provisions on security of the decision No 2015/444/EC, UE, Euratom.

  An additional marking may be attached for information at this level of security identifying the categories of persons or bodies that are the recipients of the information or authorised to access it.

- **Integrity / Availability**: Information systems and the information processed therein shall also be identified according to their level of integrity and availability, by the system owner, on the basis of the likely consequences that a loss of integrity or availability might have for the interests of the Commission, other Institutions, Member States or other parties.

  The levels are as follows:

  - **MODERATE** shall apply to information or information systems the loss of whose integrity or availability might threaten the internal working of the Commission; cases would include the non-application of the Commission's Rules of Procedure without any outside impact or with limited outside impact, a threat to the achievement of the objectives of an action plan, or the appearance of significant organisational and operational problems within the Commission without any outside impact;
  - **CRITICAL** shall apply to information or information systems the loss of whose integrity or availability might threaten the position of the Commission with regard to other Institutions, Member States or other parties; cases would include damage to the image of the Commission or of other Institutions in the eyes of the Member States or the public, a very serious prejudice to legal or natural persons, a budget overrun or a substantial financial loss with very serious adverse consequences for the Commission's finances;
  - **STRATEGIC** shall apply to information or information systems the loss of whose integrity or availability would be unacceptable to the Commission, to other Institutions, to Member States to other parties because it might, for example, lead to the halting of the Commission's decision-making process, an adverse effect on important negotiations involving catastrophic political damage or financial losses, or the undermining of the Treaties or their application.

    The minimum security requirements for STRATEGIC information are out-of-scope of this document.

1.3. Responsibility for security requirements

The Project Owner or System Owner is responsible for:

- applying the security requirements to the project and allocating financial, technical and human resources as required for meeting the security requirements of the project
- ensuring that the security controls are tested and validated during acceptance test phase
- maintaining the security controls throughout the life cycle of the product or the application

Where the security functionality in a proposed product does not satisfy specific security requirements then the risk introduced must be evaluated and additional controls must be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this must be disabled or the proposed control structure must be reviewed to determine if advantage can be taken of the available enhanced functionality.

Design reviews must be conducted at periodic intervals during the development process to assure that the proposed design will satisfy the functional and security requirements specified by the owner.

Decisions not to implement security controls or to implement alternative controls, must be subject to formally documented exemption describing the residual risks. The exemption approval process must include the System Owner and the Publications Office LISO (Local Informatics Security Officer).

2. APPLICATION-LEVEL SECURITY

In addition to the security requirements that are specified in this chapter, the contractor is also encouraged to reference and take into consideration DIGIT's document on ***"Web applications secure development guidelines"*** (DIGIT A3 – ISIP). In this document more technical issues regarding application level security are identified and addressed by presenting the main types of vulnerabilities and suggesting related countermeasures.

2.1. Identification, Authentication, Authorization

2.1.1 Web applications

- User access control rules must define what types of users can access the system, and what functions and content each of these types of users should be allowed to access must be documented and enforced.
- USER_ID's can only be used to identify and reference users and not as proof of identity or authentication mechanism.
- Access control checks to access protected URL must not be bypassable by a user that simply skips over the page with the security check.
- Administrator access through the front door of the site must not be at all possible.
- All user account management functions must require re-authentication even if the user has a valid session id.
- For accessing URL containing ""LIMITED"" information, users must be uniquely identified and authenticated with a password according to the following policy:
    - Password must be forced: :
        - to contain at least 10 characters,
        - to be a mixture of at least 3 of the following character classes:
            - upper case letters (A .. Z),
            - lower case letters (a .. z),
            - digits (0 .. 9),
            - punctuation characters (~!@#$%^&*()_+`-={}[]|\:";'<>,.?/)
        - to be different from the USER_ID (also reversed, capitalized, doubled …),
    - To prevent a reuse of the same passwords or similar passwords, a password history must be maintained. The system must memorise the last 3 passwords, and accept only a new password which differs from the 3 previous ones.
    - An account must be locked after 3 erroneous user authentication attempts and be locked for an undefined period.
    - A password reset procedure must be defined. The actual password reset may only be done by the system manager.
        - the reset procedure must include out-of-band steps to re-authenticate the user. For example, such procedure might be to request the user to answer to some specific and personalised questions, whose answers were provided during the USER_ID initialisation phase,
        - the new password must be one-time usage,
        - if the new password is sent to the user e-mail address, than the user must introduce twice the e-mail address for validation.

    - Passwords must not be stored in the application system, but only a non-reversible hash of it. Passwords should never be hardcoded in any source code or executable.
- Repeated failed login attempts must be logged.
- The system should not indicate whether it was the username or password that was wrong if a login attempt fails.
- Users should be informed of the date/time of their last successful login and the number of failed access attempts to their account since that time.
- A "change password" function must be implemented. Users should always be required to provide both their old and new password when changing their password.
- Authentication and session data should never be submitted as part of a GET, POST should always be used instead. Authentication pages should be marked with all varieties of the no cache tag to prevent someone from using the back button in a user's browser to backup to the login page and resubmit the previously typed in credentials. Many browsers now support the autocomplete=false flag to prevent storing of credentials in autocomplete caches.

2.1.2 Back-office applications

Access to the Publications Office systems and application is subject to a formal authorization procedure (DMA – Demande d'Accès) operated by the Control & Security section. The procedure is supported by a Work Flow, "suivi3D".

- When a new application is developed and rolled-out, its access control must be integrated in the DMA access control management system, by updating the DMA Applications database.
- User access authorisation approvers must be designated by the system owner.
- The application must support the USER_ID convention, as integrated in the Publications Office Active Directory and the Publications Office password security rules.
    - USER_ID convention: <five first letter of family name><two first letters of first name>
    - Password management rules:
        - The initial password must be one-time usage.
        - Password must expire automatically at the end of a period of 90 days. The period restarts at each new change.
        - Seven days before the end of the password validity period (90 days), a warning must be sent to the user after login to remind him that his password will expire. The user must be invited to change it.
        - If the user is away while the password period expires, on his return, at the first login, he is forced to change his password before continuing.
        - To prevent a reuse of the same passwords or similar passwords, a password history must be maintained. The system memorises the last 3 passwords, and accepts only a new password which differs from the 3 previous ones.
        - Password must be forced: :
            - to contain at least 10 characters,
            - to be a mixture of at least 3 of the following character classes:
                - upper case letters (A .. Z)
                - lower case letters (a .. z)
                - digits (0 .. 9)
                - punctuation characters (~!@#$%^&*()_+`-={}[]|\:";'<>,.?/)
            - to be different from the USER_ID (reversed, capitalized, doubled)
        - An account must be locked after 3 erroneous user authentication attempts and be locked for an undefined period.

- Passwords can only be reset by a system manager, upon request to the help desk.
- Passwords must not be stored in the application system, but only a non-reversible hash of it.

2.2. Input data validation

2.2.1 Web applications

- Web application and publicly available systems must not handle EU CLASSIFIED data.
- Each Web applications input data from HTTP requests must be checked against a strict format that specifies exactly what input will be allowed. All headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) must be "positively" validated against a rigorous specification that defines:
    - data type (string, integer, real, etc…)
    - allowed character set
    - minimum and maximum length
    - whether null is allowed
    - whether the parameter is required or not
    - whether duplicates are allowed
    - numeric range
    - specific legal values (enumeration) and specific patterns (regular expressions)
- Input checks must be performed at server side. On top of the server side checks, client side checking can also be included to enhance the user experience for legitimate users and/or reduce the amount of invalid traffic to the server.
- A 'positive' security check that specifies what is allowed must be implemented. "Negative" approaches that involve filtering out certain bad input or approaches that rely on signatures are not effective and are difficult to maintain.
- Direct access to files and database must be positively filtered (in URL, system calls, shell commands) against the user's rights.
- Raw data modifications in databases must not be possible. Add, modify, and delete procedures must be implement to changes data.
- Only files that are specifically intended to be presented to web users must be marked as readable using the Operating System's permissions mechanism, most directories should not be readable, and very few files, if any, may be marked executable.
- Mechanisms, including HTTP headers and meta tags, must be used to be sure that pages containing sensitive information are not cached by user's browsers.
- Protection against injection flaws must be implemented. The simplest way to protect against injection is to avoid accessing external interpreters. For many shell commands and some system calls, there are language specific libraries that perform the same functions. Using such libraries does not involve the operating system shell interpreter, and therefore avoids a large number of problems with shell commands.
    - For those calls that must be used, such as calls to backend databases, the input data must be validated to ensure that it does not contain any malicious content.
    - The use of stored procedures or prepared statements will provide significant protection, ensuring that supplied input is treated as data, and not as active commands such as SQL statements.

- Web servers must not run as ROOT or access a database as DBADMIN, otherwise an attacker can abuse these administrative privileges granted to the web application. Instead, it must run with only the privileges it absolutely needs to perform its function.
- The Java sandbox must used, when feasible, to prevent the execution of system commands.
- If an external command must be used, any user information that is being inserted into the command must be checked. Mechanisms must be put in place to handle any possible errors, timeouts, or blockages during the call.
- All output, return codes and error codes from the call must be checked to ensure that the expected processing actually occurred.

- Session management:
  - Web applications must establish sessions to keep track of the stream of requests from each user.
  - Session IDs chosen by a user should never be accepted.
  - A connection time-out must be implemented on ""CRITICAL"" (or above) applications.
  - For ""CRITICAL"" (or above) applications, the user's entire session must be protected via SSL/TLS, based on at least 192-bit 3DES (or equivalent) or 2048-bit RSA (or equivalent) digital signatures.
  - For ""MODERATE"" applications, the user's entire session should be protected via SSL/TLS. If SSL/TLS is not used, then session IDs themselves must:
    - never be included in the URL as they can be cached by the browser, sent in the referrer header, or accidentally forwarded,
    - be long, complicated, including random numbers that cannot be easily guessed,
    - must be changed when switching to SSL/TLS, authenticating, or other major transitions.
- Protections against Denial of Service attacks must be implemented
  - Application's session data must be as small as possible.
  - Resources allocated to any user must be limited to a bare minimum.
  - For authenticated users:
    - quotas should be used to limit the amount of load a particular user can put in the system,
    - one request per user should be handled at a time by synchronizing on the user's session,
    - any request being currently processed for a user should be dropped when another request from that user arrives.
  - For unauthenticated users, any unnecessary access to databases or other expensive resources must be avoided by:
    - architect the flow of the web site so that an unauthenticated user will not be able to invoke any expensive operations,
    - cache the content received by unauthenticated users instead of generating it or accessing databases to retrieve it.

2.2.2 Back-office applications

- Data input must be done via menu and selection in a list.
- If the input is captured from key string then the format and syntax must be controlled by the application to reduce the risk of errors and to prevent classical attacks such as buffer overflow and code injection. Boundary checks or field limits to specific ranges of input data must be implemented to detect the following errors:
  - out-of-range values,
  - invalid characters in data fields,

- missing or incomplete data,
- exceeding upper and lower data volume limits,
- unauthorized or inconsistent control data.

- Raw data modifications in databases must not be possible. Add, modify, and delete procedures must be implement to changes data.

2.3. Control of internal processing

- Procedures and checks must be implemented:
  - to prevent programs running in the wrong order or running after failure of prior processing,
  - to recover from failures to ensure the correct processing of data,
  - to ensure integrity of data, records files or software downloaded, or uploaded, between computers (e.g. hash code).
- reconciliation control counts to ensure processing of all data,
- Web applications must avoid implicit trust between components whenever possible. Each component should authenticate itself to any other component it is interacting with unless there is a strong reason not to (such as performance or lack of a usable mechanism). If trust relationships are required, strong procedural and architecture mechanisms should be in place to ensure that such trust cannot be abused as the site architecture evolves over time.

2.4. Error Handling

Error handling mechanisms must be able to gracefully handle any feasible set of inputs, any errors that can be generated by internal components such as system calls, database queries, or any other internal functions.

- When errors occur, the site should respond with a specifically designed result that is helpful to the user without revealing unnecessary internal details.
- Error messages must be produced and logged so that their cause, whether an error in the site or a hacking attempt, can be reviewed.

2.5. Cryptographic controls

Usage of cryptography is subject to the European Commission policy and isolated or local implementations are not authorized to avoid loss of unrecoverable encrypted data, loss of operational performance and/or law infringement. The Publications Office must only use cryptographic tools provided and supported by the European Commission which provide protection against:

- insecure storage of keys, certificates, and passwords,
- improper storage of secrets in memory,
- poor sources of randomness,
- poor choice of algorithm,
- attempting to invent a new encryption algorithm,
- failure to include support for encryption key changes and other required maintenance procedures.

2.6. Documentation and procedures

- Documented procedures must be prepared for each system activities. All information processing system documentation must be released to the system owner, with access limited to the operators. The system documentation must be classified at the same level as the system itself.
- System documentation must be assessed in terms of information confidentiality. In each document, all technical descriptions, figures, tables, architectural designs, etc. comprising confidential or business critical information (e.g. network topology, IP addresses, physical location of information resources) that only stakeholders of the contract should be able to access, must be grouped together and put in one single chapter of the system documentation. This chapter must be classified as confidential and be provided separately as annex, including all necessary cross-references as appropriate for the production of robust and complete, while at the same time properly protected, system documentation.
- The operating procedures must specify the instructions for the detailed execution of each job including, amongst others:
  - start-up and close-down procedure, including interdependencies with other systems, earliest job start and latest job completion times,
  - processing and handling of information, including scheduling requirements,
  - instruction for media handling,
  - backup,
  - equipment maintenance,
  - support contacts in the event of unexpected operational or technical difficulties,
  - instructions for handling events or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities,
  - system restart and recovery procedures for use in the event of system failure,
  - the management of log file.

2.7. e-Commerce

Electronic commerce must be protected against fraudulent activity, contract dispute and disclosure or modification of information.

The risks must be assessed and the following considerations must be taken into account:

- the level of confidence each party requires in each other's claimed identity, e.g. through authentication in line with the authorization processes associated with who may issue or sign key trading documents,
- the requirements for confidentiality, privacy, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of tendering and contracts,
- documented agreement which commits both parties to the agreed terms of trading, including details of authorization,
- compliance with all European directives and applicable international, national, regional and local laws, such as all tax acts, trade practices, Sale of Goods (or similar) acts, and so on.

If the Publications Office implements further electronic commerce facilities with on-line payment and financial transactions, then the risks must be reassessed including:

- the level of trust required in the integrity of advertised price lists,
- the level of protection required to maintain the confidentiality and integrity of order information,
- the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts,

- the degree of verification appropriate to check payment information supplied by a customer,
- the liability associated with any fraudulent transactions,
- the insurance requirements.

All e-commerce payments by credit cards must comply with the Payment Card Industry Data Security Standard (PCI-DSS), as well as the merchant agreement. The requirements are:

- Build and maintain a secure network:
  1. Install and maintain a firewall configuration to protect data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data:
  3. Protect stored data
  4. Encrypt transmission of cardholder data and sensitive information across public networks
- Maintain a Vulnerability Management Program:
  5. Use and regularly update anti-virus software
  6. Develop and maintain secure systems and applications
- Implement Strong Access Control Measures:
  7. Restrict access to data by business need-to-know
  8. Assign a unique ID to each person with computer access
  9. Restrict physical access to cardholder data
- Regularly Monitor and Test Networks:
  10. Track and monitor all access to network resources and cardholder data
  11. Regularly test security systems and processes
- Maintain an Information Security Policy:
  12. Maintain a policy that addresses information security

2.8. Logging

- Application logs must be enabled 24 hours per day, 7 days per week and kept for an agreed period to assist in case of future investigations and access control monitoring
- The following events must be logged:
  - failed or rejected user authentication and access control policy violation,
  - failed or rejected user action,
  - use of system utilities,
  - all activities performed by high level privileges accounts (System administrators, system operators) amongst others:
    - system start-up and stop,
    - changes, or attempt to change, configuration and security settings.
- Logs are classified as ""CRITICAL"" information and must be managed accordingly.

2.9. Clock synchronization

- The applications' clock must be synchronised with the OP master clock.

3. SYSTEM-LEVEL SECURITY

3.1. System isolation

- "CRITICAL" applications must be running in dedicated computing environment, possibly implemented by virtual partitioning of the same physical system.

3.2. System configuration hardening

- All applications must be able to run on the standardised Publications Office production servers configured to only offer functionality that is absolutely necessary for the provision of the envisaged service. The Service Provider must exhaustively specify the required operating system functionality, network services and security parameters.
- Software must be controlled and checked to protect against possible covert channels and Trojan code. The Publications Office applies the European Commission provided policy and settings to manage and control Java applets, Active-X controls and Java scripts.
    - **Permitted**:
        - Java applets which are downloaded from the Internet and executed in a "sandbox".
        - Java applets which are certified by an organisation inside the Commission or by an external one that is recognised by the Commission. It is advisable to add the certificates of these organisations in the certification organisation database of the Internet browsers.
    - **May be permitted, depending on risk-needs evaluation**:
        - Active-X controls that are certified by an organisation inside the Commission or by an external one that is recognised by the Commission**.**
    - **Not permitted**:
        - Unsigned Java applets which are downloaded from the Internet and installed locally.
        - Java applets *which are certified by an external organisation that is not recognised by the Commission*.
        - Active-X controls that are unsigned or certified by an external organisation that is not recognised by the Commission.
- Deviations from the standardised Publications Office servers configurations and settings must be documented and agreed with the system owner and by the Publications Office LISO.

3.3. System utilities

All unnecessary system software, compilers, editors, and other development tools or system utilities are removed from the standardized Publications Office production servers.

- If the utilization of some system utilities is required for operational reasons, the utilization if the system utilities must be:
    - subject to a formal authorization from the system owner and the Publications Office's LISO,
    - limited to a minimal number of trusted authorized individuals,
    - logged.

3.4. Development, test and production systems

- Development, test and production software must run on different systems.
- Test and development software should run on either physically separated systems or different virtual partitions.
- The test system environment should emulate the production system environment as closely as possible.
- Production data or files including 'LIMITED' information, or private data should not be used to test applications software. If, for operational reasons, the test harness is constructed from production data:
    - then those data or files must be anonimised and declassified as '"PUBLIC"' information,
    - or the test system must be classified as 'LIMITED' and the same security controls must be applied as in the production environment.
- Prototypes must not be used in production.

3.5. Security system acceptance tests

- Prior to placing a system into operation, the Publications Office will verify that the required user functions are being performed completely and correctly, and that the technical, procedural and physical security controls are operational as per these security requirements.
- The security system acceptance procedure must include tests of:
    - all security related features of the information systems,
    - secure web server configurations,
    - resilience test against the applicable vulnerabilities:
        - OWASP Top Ten Web application vulnerabilities,
        - SANS Top Twenty vulnerabilities.
- If the application is due to handle private data, then the Publications Office will check that those private data are handled according to the local jurisdiction (e.g. the CNPD in Luxembourg) and in accordance to the European Commission directive EC45/2001.
- It is the responsibility of the project owner to obtain such assurance by requesting the organization of tests and reviews with the assistance of the IT Security LISO team.

4. NETWORK-LEVEL SECURITY

- Every implementation of a new information system must be requested by the “Demande Matériel Informatique" (DMI) procedure and approved by the Publications Office IRM (Information Resources Manager).
- The servers running "CRITICAL" applications should be isolated from network segments of higher sensitivity in order to prevent attackers from using them as a platform for mounting attacks on systems in other segments.
- Connection of information processing systems to the Publications Office network must be performed by the Network section.
- Connection of workstation or information systems not owned by the Publications Office, such as contractor's PC, is not allowed.
- Remote access to the Publications Office information systems:
    - by third party users (e.g. printers) or Services Providers (e.g. remote system managers) is done by Virtual Private Network (VPN). Leased line access (with all cost always covered by the contractor) is subject to exceptional agreement after appropriate investigation.
    - Should the tenderer, during the performance of the tasks which are the subject of the Framework contract, need remote access to any communication and information system of Commission or data sets processed therein, he shall be requested to comply with security rules referred to in Article 6(5) of the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017. This entails prior authorisation which shall be granted on the basis of a formal request for network access service "Remote Access for Companies" and approval process which takes in average 4-6 weeks. The outcome of the approval, i.e. the security convention, shall be valid for a specified duration linked to the contract and shall be obtained before the connection is activated. The formal request is initiated by the concerned DG or service of the Commission and based on the risk assessment with the focus on nature and sensitivity of the tasks to be performed remotely and the security needs of each accessed communication and information system.
    - During the authorisation process the tenderer is asked to describe relevant organisational, physical, logical and network security measures in order to provide reasonable assurance that the risks are adequately and systematically covered at a level equivalent to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017, its implementing rules and corresponding security standards. The authorisation process may lead to the refusal or impose additional security requirements as a prerequisite for approval, in order to protect the Commission's communication and information system and networks from the risks of unauthorised access or other security breaches.

5. PHYSICAL SECURITY

5.1. Access to the building by non-statutory staff

Access to the Publications Office buildings by contractor's staff must be controlled in line with the Publications Office physical access control rules:

- All non-statutory staff at the Publications Office are primarily under the responsibility of the unit they are placed in. Each member of contractor's staff working at the Publications Office premises has to sign an individual non-disclosure declaration. After signature, each member of contractor's staff will be provided with a building access card for intra-muros external staff, under the following rules:
    - presence must be minimum 3 days/week for a minimum duration of stay of 2 weeks
    - validity is from date of entry until end of the year
    - the card may be taken out of the premises
- Everyone must visibly wear his/her identification card in the Publications Office buildings. It is recommended not to wear it outside the building so as not to attract undue attention.

5.2. Within the building

The Publications Office applies a clear desk and clean screen policy:

- Everyone, including contractor's staff is responsible for maintaining his working environment clear and tidy. Everyone is encouraged to avoid:
    - eating or drinking close to any IT equipment not to damage the equipment;
    - leaving any non-business related information or equipment in the office.
- All paper based information which is not "PUBLIC" and any removable storage media or device must be locked in a closed cabinet at the end of the working day or when the office is not attended.
- It is the responsibility of everyone to ensure all obsolete "PUBLIC" paper based information is sorted in the dustbin foreseen for "paper to recycle".
- It is recommended to use local paper shredder to dispose obsolete "LIMITED" paper based information and zeroisation techniques to securely erase all storage media.
- The Publications Office does not allow removing its properties out of its buildings.

5.3. Operations outside the building (outsourced)

- Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. Operating centres must be equipped with blind and shielded windows.
- All offices and computer rooms must be equipped with regularly tested UPS outlets.
- All power and data cables must be laid down in separate cable trays.
- All equipments must be maintained in accordance with the equipment provider's recommended service intervals and specifications. Only authorized maintenance personnel must carry out repairs and service equipment. Records must be kept of all suspected or actual faults, and all preventive and corrective maintenance. All requirements imposed by insurance policies must be complied with.

6. EXPLOITATION-LEVEL SECURITY

6.1. Change Management

The Publications Office production systems are subject to strict change control management.

- All patches and service packs must be tested and validated before promotion to production.
- Automated updates must not be used as some updates may cause applications to fail.
- The decision to install changes in production is taken by the system owner. Installation is typically performed after business hours; otherwise the service interruption procedure must be used in agreement with the infrastructure production manager.

6.2. Business Continuity Management

The Publications Office has developed a comprehensive Business Continuity Management framework, supported by disaster recovery plan.

- The target system must be integrated into the Publications Office BCM framework.
- A copy of the accepted production server content must be safe stored in a location distinct from the production site.

7. THIRD PARTIES' OBLIGATIONS

7.1. Adherence to the BISP

- All contractor's staff working at the Publications Office are required to comply with the BISP and its supporting practices and baselines.

7.2. Non-Disclosure Agreement

- Any information, data and/or materials of whatever kind or nature that is transmitted to the contractor related to the Publications Office shall be considered as "LIMITED" and proprietary to the Publications Office, unless explicitly released as "PUBLIC" information and must be treated as such by the Service Provider.
- The "LIMITED" information may also include information which has been submitted to the Publications Office by third parties, and which the Publications Office has been authorised to disclose, subject to security measures or confidentiality provisions. In such case, the contractor accepts that the terms of the service agreement shall be deemed to be also for the benefit of the Publications Office and any such third parties and fully binding upon the contractor with respect to such "LIMITED" information.
- The contractor shall neither use nor copy the "LIMITED" information for any purpose other than the execution of the service agreement and shall neither directly nor indirectly disclose or permit such "LIMITED" information to be made available to any third party without prior written authorization from the Publications Office system owner or the Publications Office LISO.
- The contractor undertakes that it will only disclose any "LIMITED" information to those of its employees, subcontractors, or any other third parties on a "need to know basis". Prior to disclosing any "LIMITED" information to any third party the contractor will:
    - inform that third party of the restrictions on the use and disclosure of the "LIMITED" information,
    - ensure that the third party is bound by a confidentiality undertaking or obligations of confidence which protect the "LIMITED" information to at least the extent that it is protected under the contractor's agreement.
- Upon the written request of the Publications Office, the contractor shall, at the Publications Office's option, promptly return or destroy all documents and other materials in whatever form containing "LIMITED" information from the Publications Office.

7.3. Third party access to Publications Office systems

- Third parties may not access the Publications Office internal processing systems unless formal contractual agreement is signed.
- Only after signature, the third party is allowed to issue access requests via the DMA procedure (Suivi3D internal tool).

7.4. Auditing & monitoring right

- At any time the Publications Office reserves the right to audit the contractor for compliance to the Publications Office BISP. Such audit should be announced in advance with a reasonable notice.
- The Publications Office has the right to monitor and examine any information stored on its information processing systems or communicated over its network or equipment.
- The Publications Office will access this information without the contractor's consent or advance notice only:
    - for capacity planning purpose,
    - for back-up and archiving purpose,
    - if there is sufficient cause or evidence indicating abuse, non respect of the BISP or the suspicion of a fraud or crime. In such case, the explicit authorization of the Publications Office LISO will be required before conducting any investigation.

7.5. Obligation of reporting

- The contractor has the obligation to report all security incidents, software malfunctions, security weaknesses or threats to systems or services that their staff notice or is made aware of to the Publications Office help desk or the Publications Office LISO.
- All users are instructed that they must not, unless formally authorized by the Publications Office LISO, attempt to prove a suspected weakness because this will be interpreted as a potential misuse of the system, could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

7.6. Other obligations

- Processing of personnal data, confidentiality, intellectual property rights, legal software copies: see the articles of the contract.