Joint Interpretation Library

Minimum Site Security Requirements

Version 1.1 (for trial use)
July 2013

Acknowledgments:

The organisations listed below and organised within the Joint Interpretation Working Group (JIWG) provide JIWG Supporting documents in order to assist the consistent application of the criteria and methods between SOG-IS Evaluation and Certification Schemes.

France:	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Germany:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Italy:	Organismo di Certificazione della Sicurezza Informatica (OCSI)
Netherlands:	Netherlands National Communications Security Agency (NLNCSA)
Spain:	Centro Criptológico Nacional (CCN)
United Kingdom:	Communications-Electronics Security Group (CESG)

They also acknowledge the contribution of the work done by several smart card vendors, evaluation labs, and other companies organised within:

- eEurope
- International Security Certification Initiative (ISCI)

Table of contents

1 Introduction

1.1 Objective

1 The Common Criteria (CC) facilitates comparability between the results of independent security evaluations. The CC provides a common set of requirements to evaluate the security functionalities of IT products and the assurance measures applied to these IT products. The CC describes in ALC_DVS what the evaluator has to examine with regard to developer security but does not define the minimum site security requirements. The evaluator is responsible to determine an acceptable set of security measures. There is a desire for harmonization on this topic by all involved parties. The purpose of this document is to define a set of minimum requirements that a developer shall meet and that an evaluator is able to verify during any type of Common Criteria evaluation in order to ensure compliance with ALC_DVS.1 and ALC_DVS.2 in a manner consistent with today's standard practices for evaluations requiring high assurance (AVA_VAN.5).

2 This document is mandatory for Common Criteria evaluation of Smartcard and similar devices, including related software development.

3 Part of the verification whether or not the implemented measures are sufficient can be performed using the documentation provided by the developer. In any case a site visit by the evaluator is indispensable.

4 The document is based on CEM paragraphs 1102ff. and CEM Annex A.4.3.2. The requirements are structured according to ISO27001. An information security management system certified according to ISO27001 is neither necessary nor sufficient to pass Common Criteria evaluation.

5 Each relevant area covered by these requirements is described in terms of objectives and a description of best practices.

6 The requirements in this document apply to environments used for the development (all steps of the life cycle until delivery) of the TOE and shall be interpreted from a TOE perspective in terms of confidentiality or integrity.

1.2 Application

7 The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size and nature. No particular requirements from a Protection Profile (PP) have been included. All CC/CEM references are from version 3.1.

8 The requirements defined in this document shall be used by the ITSEF to create a checklist to prepare the examination

9 The requirements are specifically aimed at an evaluation of EAL4+ and higher where the attacker has a high attack potential (AVA_VAN.5). The criteria can be used from EAL3 upwards as it is at this level that ALC_DVS first appears in the assurance criteria. In all cases, the attack potential of the threat agent should be considered when determining if the deployed measures are sufficient. The evaluator shall also consider the organizational security policies (OSP) and assumptions of the Security Target.

10 The developer has to consider all the controls specified in this document in order to pass site security evaluation. Any exclusion of controls needs to be justified and shown not to affect the developer's ability, and/or responsibility, to provide a level of security that meets the security objectives defined in this document.

11 If all applicable requirements from this document are implemented through appropriate measures in a meaningful way the CC work units for ALC_DVS are fulfilled (except in very particular cases). In that case the developer can refer to this document in order to justify that the measures maintain confidentiality and integrity.

12 The examples in this document describe the expected and preferred security measures. If the developer implements a different security setup he has to ensure and demonstrate that at least the same level of security is achieved.

2 Normative references

13 The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- Common Criteria for Information Technology Security Evaluation, Part 1-3, September 2012, Version 3.1 Revision 4
- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1 Revision 4
- ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management

14 The following standards may be beneficial in implementing the respective processes.

- ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27005:2008, Information technology - Security techniques - Information security risk management

3 Terms and Definitions

15 For the purposes of this document, the following terms and definitions apply.

Assets	entities that the owner of the TOE presumably places value upon; in context of the Development Security System assets are information in electronic or other form, information processing facilities and referring processes (incl. access control and alarm systems), development tools and environments, any manifestation of the TOE, and customer code & data provided to produce the TOE
Availability	the property of being accessible and usable upon demand by an authorized entity
Business operations	is the general term for the entirety of operations performed by the developer relate to the TOE, e.g. "personalization" is part of business operations

CC	Common Criteria for Information Technology Security Evaluation, Part 1-3, July 2012, Version 3.1
Confidentiality	the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Control	Set of measures associated to an objective
Data processing facilities	premises, equipment, installation or tool used for data processing
Developer	Entity (Site) offering services and being part of the development and production process; this encompasses all steps of the life cycle until delivery to the customer, e.g. software development, chip design, mask making, wafer production, testing, assembly etc. The developer is also responsible for supporting functions
Development environment	Environment in which the TOE is developed; development includes the production of the TOE
DMZ	Demilitarized Zone; in computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet
DSD	Development Security Document
DSS	Development Security System
Employment	The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.
Evaluation	assessment of a PP, an ST or a TOE, against defined criteria
Evaluation assurance level	set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Evaluation authority	body that sets the standards and monitors the quality of evaluations conducted by bodies within a specific community and implements the CC for that community by means of an evaluation scheme
Evaluation scheme	administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community
Facility	any equipment, installation or tool, regardless of being software or hardware, which is part of the security management system

Information security (IS)	preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
Integrity	the property of safeguarding the accuracy and completeness of assets
IS event	an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
IS incident	a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
ISMS	Information Security Management System
Mobile Computing	Data processing on a mobile device
Organization	group of people and facilities with an arrangement of responsibilities, authorities and relationships
Organizational Security Policy	set of security rules, procedures, or guidelines for an organisation
Owner	The term owner identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term owner does not mean that the person has any property rights to the asset
Partner	Any organization which has been part of the supply chain within the past two years, e.g. development company, mask house, production site, test floor, assembly line, regardless of their ownership
PP	Protection Profile, an implementation-independent statement of security needs for a TOE type
Procedure	A specified way to perform an activity
Process	A sequence of activities or procedures
Reliability	The ability of either a facility or a procedure to perform a required function over time
Remote access	Connection to a data processing system from a location off premises by means of a network connection where - the connection is from outside the logical security environment - the working location is outside the physical security environment
Residual risk	the risk remaining after risk treatment

Risk acceptance	decision to accept a risk
Risk analysis	systematic use of information to identify sources and to estimate the risk
Risk assessment	overall process of risk analysis and risk evaluation
Risk evaluation	process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk management	coordinated activities to direct and control an organization with regard to risk
Risk treatment	process of selection and implementation of measures to modify risk
Sensitive data	Data which needs protection in order to support confidentiality and/or integrity requirements
ST	Security Target, an implementation-dependent statement of security needs for a specific identified TOE
Strong authentication	Authentication with at least two independent factors, e.g. possession and knowledge (badge and PIN), or possession and individual attribute (badge and biometrics)
Teleworking	Working via remote access
Threat	Any circumstance or event with the potential to adversely impact organizational operations, assets (incl. TOE or its parts), or individuals via unauthorized access, destruction, disclosure, modification, and/or denial of service. Also, the potential for a threat-source to successfully exploit particular system vulnerability. The Common Criteria characterizes a threat in terms of (a) a threat agent, (b) a presumed method of attack, (c) any vulnerability that is the foundation for the attack, and (d) the system resource that is attacked.
Top Management	The highest ranking executives (with titles such as chairman/chairwoman, chief executive officer, managing director, president, executive directors, executive vice-presidents, etc.) responsible for the entire enterprise. In organizations where the developer is not the only activity “Top Management of the developers’ organization” may refer to the management of a division, business group, product line etc.
TOE	Target of Evaluation, a set of software, firmware and/or hardware possibly accompanied by guidance

16 ISO terminology, such as "can", "may", "normative", "shall" and "should" used throughout the document are defined in the ISO/IEC Directives, Part 2. Note that the term "should" and “informative” have an additional meaning applicable when using this standard. See the note below.

17 The word “shall” indicates measures strictly to be followed in order to conform to the document and from which no deviation is permitted.

18 The word “should” indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. The CC interprets “not necessarily required” to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

19 The word “may” indicates a course of action permissible within the limits of the document.

20 The word “can” is used for statements of possibility and capability, whether material, physical or causal.

21 The expression “confidentiality and/or integrity” means either “confidentiality” or “integrity”, or a combination of both.

22 The expression “informative” indicates measures that are not mandatory to follow in order to conform to the document.

4 Development security documentation

4.1 General requirements

23 Development security is concerned with physical, logical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE and its parts. It includes the physical security of the development and production location(s) and any procedures used to select development and production staff.

24 Security-specific impairment commonly includes, but is not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset authenticity.

25 Consistently with §1082 – 1097 of CEM the objective is to determine whether the developer’s security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised.

26 The threats to be covered by appropriate security measures include

- "Accidental threat": A possibility of human error or omission, unintended equipment malfunction, or natural disaster.
- "Intentional threat": A possibility of an attack by an intelligent entity (e.g. an individual hacker or a criminal organization). Examples for such attacks are theft and pilferage, intentional exchange of the TOE or its parts, and cloning.

27 The developer shall provide development security documentation (DSD)

28 The developer shall establish, implement, operate, monitor, maintain, review, and improve a documented Development Security System (DSS) within the context of the organization's overall business activities and the risks it faces.

29 As required by ALC_DVS.1.1C the development security documentation shall describe the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

30 It shall identify the locations where development occurs, the development activities, and the security measures applied at each location linked to such activities and for transports between different locations.

31 If ALC_DVS.2.2C is claimed the development security documentation shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE according to the attack potential claimed in the ST (AVA_VAN.5). In that case justification may refer to this document.

4.2 Establishing and managing the DSS

32 CEM ALC_DVS.1-2 requires the evaluator to examine the development confidentiality and integrity policies in order to determine the sufficiency of the security measures employed.

4.2.1 Establish the DSS

33 The establishment of the DSS is mandatory for the developer. It is common practise to define the scope and boundaries of the DSS with respect to the characteristics of the organization, its location, assets and technology, and including details of and justification for any exclusion from the scope.

34 The developer

a) should define a Security Policy that includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to the integrity and confidentiality needs of the TOE.

b) may define the risk assessment approach of the organization including a risk assessment methodology that is suited to the DSS, the identified security, legal and regulatory needs to protect the TOE,

35 Note: Risk assessment is intended to identify, analyse and evaluate risks, identify, evaluate, and select control objectives and controls for the treatment of risks, and produce comparable and reproducible results.

36 Control objectives and controls should be selected, implemented, and documented to meet the requirements identified by the developer.

37 The control objectives and controls described in this document are not exhaustive and additional control objectives and controls may also be selected.

4.2.2 Implement and operate the DSS

38 The organization

a) may formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing security risks.

b) may implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.

c) should implement the controls selected to meet the control objectives.

d) may define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results.

e) should implement training and awareness programmes.

f) should manage operation of the DSS.

g) should manage resources for the DSS.

h) should implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents.

4.2.3 Monitor and review the DSS

39 The organization

a) should execute monitoring and reviewing procedures and other controls to:

1) promptly detect errors in the results of processing;

2) promptly identify attempted and successful security breaches and incidents;

3) enable management to determine whether the security activities delegated to people or implemented by technology are performing as expected;

4) help detect security events and thereby prevent security incidents by the use of indicators; and

5) determine whether the actions taken to resolve a breach of security were effective.

b) should undertake regular reviews of the effectiveness of the DSS taking into account results of security audits, incidents, results from effectiveness measurements, and suggestions and feedback from all interested parties.

c) may review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks.

d) should conduct internal DSS audits at planned intervals defined in DSD.

e) should update security plans to take into account the findings of monitoring and reviewing activities.

f) should record actions and events that could have an impact on the effectiveness or performance of the DSS.

4.2.4 Maintain and improve the DSD

40 In order to ensure the DSD is up to date the developer regularly

a) should implement the identified improvements of the DSS in the DSD.

b) should take appropriate corrective and preventive actions in accordance with 8.2 and 8.3.

c) may apply the lessons learnt from the security experiences of other organizations and those of the organization itself.

d) should communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.

4.3 Documentation requirements

4.3.1 General

41 The DSD should include:

a) documented statements of the DSS policy and objectives;

b) the scope of the DSS as far as TOE is concerned;

c) procedures and controls in support of the DSS;

d) documented procedures needed by the organization to ensure the effective planning, operation and control of its developer security processes.

42 It might be helpful for justification to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the DSD policy and objectives.

4.3.2 Control of documents

43 Documents required by the DSS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

a) approve documents for adequacy prior to issue;

b) review and update documents as necessary and re-approve documents;

c) ensure that changes and the current revision status of documents are identified;

d) ensure that documents remain legible and readily identifiable;

e) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification;

f) prevent the unintended use of obsolete documents; and

g) apply suitable identification to them if they are retained for any purpose.

4.3.3 Control of records

44 Records shall be established and maintained to provide evidence of conformity to requirements, including the effective operation of the DSS. They shall be appropriately protected and controlled. Records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.

45 Records shall be kept of the operation of the processes and of all occurrences of significant security incidents related to the DSS.

5 Management responsibility

5.1 Management commitment

46 Top Management (see 3) should support establishment, implementation, operation, monitoring, review, maintenance and improvement of the DSS, at least by assigning one or more people to the role of Security Manager and providing necessary resources.

47 The Security Manager(s) shall be responsible for overall security within the developers' area of responsibility throughout the whole development life cycle of the TOE, including any subcontractors that may be used. In this function, the Security Manager should report to the Top Management of the developers' organisation. The objectives and task of the Security Manager shall include but are not limited to the requirements listed in 4.2 and 4.3.

5.2 Resource management

48 All roles and responsibilities involved with developers' activities shall be well defined and documented, e.g. work-flows, role descriptions, org-chart.

49 It is good practice to implement organizational measures to ensure segregation of duties between development, production, testing, quality assurance, and security.

5.2.1 Provision of resources

50 The organization shall determine and provide the resources needed to satisfy the requirements listed in 4.2 and 4.3.

51 A management authorization process for new information processing facilities potentially impacting the TOE security may be defined and implemented.

5.2.2 Training, awareness and competence

52 The organization shall ensure that all personnel who have been assigned responsibilities defined in the DSS are competent to perform the required tasks by:

a) determining the necessary competencies for personnel performing work effecting the DSS;

b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;

c) evaluating the effectiveness of the actions taken; and

d) maintaining records of education, training, skills, experience and qualifications.

53 The organization shall ensure that all relevant personnel, including members of external parties, are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the DSS objectives.

5.2.3 Confidentiality agreements

54 Requirements for confidentiality or non-disclosure agreements reflecting the developer's needs for the protection of information, data, and material shall be identified and regularly reviewed.

5.2.4 External parties

55 Even in the case where the organization's premises and processing facilities are accessed, processed, communicated to, or managed by external parties, the security shall be maintained.

56 Developer is responsible for all premises used even if they are owned by a third party unless the site has an appropriate CC site certification.

5.2.4.1 Identification of risks related to external parties

57 Cooperation with external parties (e.g. customers, development partners, production partners, vendors, suppliers, carriers, evaluation bodies) is inevitable. The risks to the developer's information, data, material, and processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting physical or logical access.

5.2.4.2 Addressing security in third party agreements

58 Agreements with third parties involving accessing, processing, communicating or managing the developer's information, data, and material in development, production and information processing facilities, or adding products or services to production and information processing facilities shall cover all relevant security requirements.

6 Internal DSS audits

59 The organization should conduct internal DSS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its DSS:

a) conform to the requirements of this Requirement Document;

b) conform to the identified security needs of the TOE;

c) are effectively implemented and maintained; and

d) are performing as expected.

60 An audit program should be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods should be defined. The

selection of auditors and conduct of audits should ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

61 The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records should be defined in a documented procedure.

62 The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities should include the verification of the actions taken and the reporting of verification results.

7 Management review of the DSS (informative)

7.1 General

63 Management may review the organization's DSS at planned intervals, or when significant changes to the security implementation occur, to ensure its continuing suitability, adequacy and effectiveness. This review may include assessing opportunities for improvement and the need for changes to the DSS. The results of the reviews should be clearly documented and records should be maintained.

7.2 Review input

64 The input to a management review may include:

a) results of DSS audits and reviews;

b) feedback from interested parties, particularly Evaluation and Certification Bodies;

c) techniques, products or procedures, which could be used in the organization to improve the DSS performance and effectiveness;

d) status of preventive and corrective actions;

e) vulnerabilities or threats not adequately addressed in the previous risk assessment;

f) results from effectiveness measurements;

g) follow-up actions from previous management reviews;

h) any changes that could affect the DSS; and

i) recommendations for improvement.

7.3 Review output

65 The output from the management review may include any decisions and actions related to:

a) improvement of the effectiveness of the DSS.

b) update of the risk assessment and risk treatment plan.

c) modification of procedures and controls that effect security, as necessary, to respond to internal or external events that can impact the DSS.

d) resources needed.

8 DSS improvement

8.1 Continual improvement

66 The developer may continually improve the effectiveness of the DSS through the use of the security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.

8.2 Corrective action

67 The developer shall take action to eliminate the cause of nonconformities with the DSS requirements in order to prevent recurrence. The documented procedure for corrective action may define requirements for:

a) identifying nonconformities;

b) determining the causes of nonconformities;

c) determining and implementing the corrective action needed;

d) recording results of action taken; and

e) reviewing corrective action taken.

8.3 Preventive action

68 The developer should determine actions to eliminate the cause of potential nonconformities with the DSS requirements in order to prevent their occurrence. The documented procedure for preventive action may define requirements for:

a) identification of potential nonconformities and their causes;

b) determination and implementation of preventive action needed;

c) reviewing preventive action taken.

69 The developer should identify changed threats and identify preventive action requirements focusing attention on significantly changed risks.

70 The priority of preventive actions may be determined based on the results of a risk assessment.

9 Control objectives and controls

71 The control objectives and controls listed below are directly derived from and aligned with those listed in ISO 27002:2005 Clauses 5 to 15. The lists are not exhaustive and a developer may consider that additional control objectives and controls are necessary.

9.1 Asset management

9.1.1 Responsibility for assets

72 Objective: To achieve and maintain appropriate protection of assets.

73 Security is involved with all kinds of assets but not all aspects of assets are in the scope of this DSS, e.g. QM (Quality Management), ESH (Environment, Safety, Health).

74 All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

75 Owners shall be identified and nominated for all assets and the responsibility for the maintenance of appropriate controls shall be formally assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

9.1.1.1 Inventory of assets

76 All assets shall be clearly identified and an inventory of all important assets drawn up and maintained. The inventory should include:

- Type of asset
- Type of protection (confidentiality, integrity, authenticity, …)
- Format
- Location
- Backup information
- License information
- protection level, criticality

77 The most important assets within the scope of this document are the TOE or parts of it. However, the form differs from segment to segment of its life cycle. Typical segments are design, production, shipment, usage, and disposal.

Example:

For a typical Smart Card product (IC manufacturer) the following segments of the life cycle and forms of the TOE apply.

- Design – security concept, layout, net plan, software, data, bond out, design doc's (ADV-class)
- Mask production – pattern data, mask data, reticle
- Wafer production – reticle, wafer
- Wafer test – wafer, test program, (flash) application, application (EEPROM) data
- Assembly – wafer, modules/chips, test program
- Card/Inlay manufacturing – modules, cards
- Personalization – cards/inlays, software, data
- Shipment – reticle, wafer, modules/chips, cards/inlays

Rejects and scrap may appear in all segments and shall be considered assets.

78 Examples of assets beside the TOE or parts of it:

a) Security: access control and alarm system, keys, access codes

b) Information: databases, data files, contracts, system documentation, R&D information, archived information, production related data

c) Software: applications, system software, development tools, CM systems

d) Physical assets: computer equipment, communication equipment, removable media

e) Services: computing and communications services, general utilities (power, air conditioning, lighting), storage and shipment

9.1.1.2 Ownership of assets

79 All information and assets associated with information processing facilities shall be owned by a designated part of the organization.

80 The owner is responsible for:

- Ensuring that information and assets associated with processing facilities are appropriately classified
- Defining and periodically reviewing access restrictions and classifications, taking into account applicable control policies.

81 Ownership may be allocated for:

- A business process
- A defined set of activities
- An application
- A defined set of data
- Physical assets (premises, HW, networks etc.)

82 All information about assets should be kept in appropriate databases.

9.1.1.3 Configuration Management System

83 According to ALC_CMC an appropriate Configuration Management System shall identify and document the functional and physical characteristics of the TOE and its parts, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements in a way relevant for the different parts of the lifecycle. The CM system shall ensure the integrity of the TOE from the early design stages through all subsequent maintenance efforts, that the TOE is correct and complete before it is sent to the consumer and preventing unauthorized modification, addition, or deletion of TOE configuration items.

84 In the design phase of the TOE a configuration list shall clearly define all configuration items for a specific product together with the exact version of each item relevant for a specific version of the TOE and its parts, thereby allowing distinguishing the items belonging to different versions of the product.

85 During manufacturing the CM system shall ensure that only the planned processes and recipes are applied, that they are applied in the correct order, and that all manufacturing steps are documented to facilitate full traceability.

86 Detailed requirements for CM systems are defined in CC part 3, ALC.

9.1.1.4 Acceptable use of assets

87 Rules for the acceptable use of information and assets associated with processing facilities should be identified, documented, and implemented.

88 All employees, contractors, and third party users shall follow developer's rules regarding acceptable use of assets. Computers and all other equipment and materials provided by the developer shall be used for official purposes only, and only according to the rules set in the DSS and related documents.

9.1.2 Classification of information, data, and material

89 Objective: To ensure that information, data, and material receives an appropriate level of protection.

90 Where confidentiality is a requirement, all relevant information, data, and material shall be classified according to an appropriate security level. The developer should apply at least four levels of security, e.g.

- open, public
- for internal use, company proprietary
- confidential, under NDA
- strictly confidential, company secret, top secret

91 The developer shall have predefined handling procedures for all defined levels.

92 Access to restricted information, i.e. classified "confidential" or "strictly confidential", shall only be granted on a need-to-know basis.

93 When a high level of security for especially critical material or operations is required, e.g. in case of classification strictly confidential, the two-man rule ("four eyes principle") should be applied as a control mechanism. Under this rule, all access and actions requires the presence of two authorized people at all times.

9.1.2.1 Classification guidelines

94 Information, data, and material shall be classified in terms of its criticality to the developer's organization and, particularly, to the intended area of application of any TOE concerned.

95 These rules relate to information, data, and material in any form, e.g.

- Speech (e.g. verbal communication, telephone, video conference)
- Writing (e.g. documents, memos, presentations, drafts)
- Electronic data (e.g. files, emails, software, development tools, CM systems, networks etc.)

- TOE and components (masks/reticules, wafer, dies, chips/modules, inlays, cards, demonstrators, samples, software etc.)

9.1.2.2 Labelling and handling of information, data, and material

96 An appropriate set of procedures for labelling and handling of information, data, and material shall be developed and implemented in accordance with the classification scheme adopted by the organization.

97 The procedures should include, but are not limited to regulations regarding

- Creation, Labelling, Issuing
- Distribution
- Dispatch / Transmission
- Retention / Storage
- Disposal / Destruction / Deletion

98 Information, data, and material classified “confidential”, “under NDA” or higher shall be protected at any time.

Example:

Confidential electronic information is:

- distributed only to a defined group of people,
- transmitted electronically with appropriate end-to-end encryption (e.g., in 2012 German BSI requires at least 80 bits of entropy, i.e. 256 bit symmetric or 2048 bit asymmetric RSA key length),
- stored as encrypted file, in a secure container or in a separated network, and
- deleted by means of a wipe tool using at least 1 pass with random data pattern.

9.1.2.3 Destruction and disposal of material

99 Finished goods, semi-finished goods, rejected material, or parts of it that contain the TOE or its parts and that are no longer needed shall be destroyed in a way that remains cannot be used in any meaningful way that might affect the confidentiality of the TOE.

Example:

Wafer, single dies, and packaged chips are shredded in a rolling mill so that every edge of each and any die is cut 3 times.

Masks/Reticules are re-etched in order to remove the pattern or shredded in a rolling mill.

The destruction process is recorded on CCTV.

Confidential and strictly confidential documentation of the TOE on paper or optical disks are shredded according to at least DIN 32757, LEVEL3 (2 mm strips or 4 x 30mm particles).

Files on re-writable data carriers (HDD, SSD, USB sticks) are wiped or destroyed as described above.

100 The related processes shall be designed to provide full traceability of every piece of any tangible form of the TOE or its parts.

9.1.3 Rules for preserving integrity and authenticity of assets

101 Objective: To ensure that information, data, and material receives an appropriate level of protection against alteration or unauthorized modification.

102 Where relevant, all information, data, and material shall be classified according to an appropriate security property level (integrity, authenticity). This applies in particular to the transfer of ROM code, EEPROM content, or software related to the TOE. The supplier should apply at least three levels, e.g.

- basic
- standard
- enhanced

103 The developer shall have predefined handling procedures for all defined levels. If no specific requirements are defined for integrity the confidentiality classification may be sufficient.

Example:

In a typical setup the level “enhanced” is used for

- ROM code during the transfer from the application developer to the chip manufacturer;
- Mask data during the transfer from chip developer to mask production.

In these cases, integrity is protected by hash values and electronic signature.

The level “standard” is used for EEPROM content which is protected by hash values.

Confidential and strictly confidential Documentation of the TOE are shredded according to at least DIN 32757, LEVEL3 (2 mm strips OR 4 x 30mm particles).

Files on hard disks, USB sticks or optical disks are wiped or destroyed as well.

104 Access to information classified “standard” and “enhanced” shall only be granted on a need to use basis.

9.2 Human resources security

9.2.1 Prior to employment

105 Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

9.2.1.1 Roles and responsibilities

106 Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's security policy, e.g. in job descriptions, project plans, contracts etc.

9.2.1.2 Screening

107 The developer shall grant access to the TOE or its parts only to trustworthy people. That objective should be accomplished by appropriate hiring and termination procedures which ensure careful selection of trustworthy staff.

108 Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant local laws, regulations and ethics, and proportional to the business requirements, the classification of the information and material to be accessed, and the perceived risks.

109 Respecting privacy regulations, the developer shall make a reasonable effort to gain confidence in the integrity of the staff, e.g. through

- careful check of applications regarding completeness, conclusiveness, and authenticity,
- check of indicated references, and
- criminal record check ("Clearance Certificate", "Criminal Records Bureau check", "Casier judiciaire", "Polizeiliches Führungszeugnis" etc.).

9.2.1.3 Terms and conditions of employment

110 As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for security.

111 Contracts with all employees (permanent, temporarily, subcontractors, students etc.) shall contain a confidentiality clause which remains valid after expiration/termination of the contract; third party users respectively shall sign a non disclosure agreement (NDA).

9.2.2 During employment

112 *Objective:* To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

9.2.2.1 Management responsibilities

113 Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

114 Developer's management is responsible to ensure that employees, contractors, business partners and third party users

a) are properly briefed on their security roles and responsibilities prior to being granted access to sensitive areas, information, or information systems;

b) are provided with guidelines to state security expectations of their role within the organization;

c) achieve a level of awareness on security relevant to their roles and responsibilities within the organization;

d) conform the terms and condition of employment, which includes the organization's information security policy and appropriate methods of working;

e) continue to have the appropriate skills and qualifications;

f) observe the rules; and

g) lead by example.

9.2.2.2 Information security awareness, education and training

115 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. That can be face to face or online training. Records of the trainings shall be kept, including date, attendances and content.

116 An Initial and regular (annual) security training programs shall make the development team members aware of their responsibilities, e.g. handling of documents and information, behaviour in public, and encourage them to act pro-actively when problems occur.

9.2.2.3 Disciplinary process

117 There should be a formal disciplinary process for employees who have committed a security breach. Violations of security rules may be punished by disciplinary measures depending on the nature and gravity of the breach and its impact on confidentiality and integrity of the TOE, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required.

118 The disciplinary process should also be used as a deterrent to prevent employees, contractors, business partners and third party users violating organizational security policies and procedures, and any other security breaches.

9.2.3 Termination or change of employment

119 *Objective:* To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

9.2.3.1 Termination responsibilities

120 Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned. This shall also apply to contracts with third party users.

9.2.3.2 Return of assets

121 All employees, contractors and third party users shall return all of the developer's assets in their possession upon termination of their employment contract or agreement. The same shall apply when they leave the developer's organization due to change of job assignment.

122 This process should be supported by a checklist for employees leaving employment in order to make sure that all relevant tasks, e.g. return of company properties, deletion of access rights are completed.

9.2.3.3 Removal of access rights

123 A process shall be in place to ensure that access rights (physical and logical) of all employees, contractors and third party users to developer's facilities shall be revoked without delay when no longer needed, particularly upon termination of their employment, contract or agreement, or adjusted upon change.

124 Access rights can include but are not limited to

- Physical access to sites, premises, buildings, rooms
- Active Directory groups
- Files, folders, network shares
- Applications
- Mailboxes
- Distribution lists
- External (remote) access to the Network

125 In case of suspension or dismissal due to disciplinary reasons access rights shall be revoked immediately. The Security Manager shall be notified.

126 Where appropriate, team members should be notified about changed access rights.

9.3 Physical and environmental security

9.3.1 Secure areas

127 *Objective:* To prevent unauthorized physical access to the organization's premises, assets, and information leading to damage to confidentiality or integrity of TOE.

128 According to CEM paragraph 1104 "Development includes the production of the TOE". CEM paragraph 1103 requires that "the development security documentation shall identify the locations at which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and for transports between different locations. For example, development could occur in different rooms within a single building, multiple buildings at the same site, or at multiple sites.

129 Transports of parts of the TOE or the unfinished TOE between different development sites are to be covered by the Development security (ALC_DVS), whereas the transport of the finished TOE to the consumer is dealt with in the Delivery (ALC_DEL)."

9.3.1.1 Physical security perimeter

130 Development areas where integrity and/or confidentiality of the TOE or its parts could be impaired shall be properly secured.

Example:

In a typical setup, the premises are located within a fenced site. The fence is protected with sensors (vibration, e.g. Perifone; motion, e.g. IR curtain, or digital CCTV).

Buildings are constructed with concrete or stonework walls, ceilings and floors, or enforced (metal grid) light construction with alarm tapestry.

Controlled doors are strong (including frames), close automatically, and are monitored with magnetic contacts and CCTV.

Windows are secured with irremovable metal grid or with magnetic contacts and glass breakage sensors.

Where the site may not be fenced an IR curtain can be deployed or the outer skin of the building is monitored by digital CCTV with motion detection ("Telemat").

131 The first protection layer of the premises shall have at least two lines of defense, a detection layer and a stop layer. These layers shall separate authorized from unauthorized people, including employees.

132 In case that no physical manifestation of the TOE or its parts is handled and solely logical access to electronic data is present a stop layer may also be a logical one.

Example:

A Detection Layer may consist of at least one of the following:

- Fence with sensor (vibration, ultrasonic, motion, etc.)
- IR curtain
- Digital CCTV with motion detection
- Wall with alarm tapestry or vibration sensor
- 24/7 guard post

A Stop Layer is a constructive measure which needs time to overcome:

- Concrete or brick stone wall
- dry walling construction enforced with inside metal grid (> 8mm diameter, < 100 mm grid distance) or enforced with steel plate (> 3mm thickness)
- windows in a stop layer are either protected with metal bars (> 8 mm diameter) or made with bullet proof glass
- door hardware must be properly installed, locked door blades fixed at floor and ceiling

133 In case buildings are not solely used for developers' activities, e.g. shared with other users from the same organization, the layers shall separate the different activities.

134 In general, the layers should provide

- perimeter protection
- protection of the outer skin of the building
- protection of the outer skin of the development area
- protection of restricted areas within the development area

135 The resistance time value of the stop layer shall exceed the reaction time of supporting forces. This should be supported by the construction.

136 All openings towards the secured development area (air condition, cable ducts, etc.) shall be protected in order to effectively prevent intrusion, e.g. with a welded metal grid.

9.3.1.2 Physical entry controls

137 Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

138 Access requests shall be submitted in written or via an electronic work flow system. Access rights shall only be granted to employees and contractors on a need-to-know basis. A process shall be in place to ensure that access rights can only be granted after approval of responsible people, e.g. the manager of the applicant, the owner of the area, and the Security Manager.

139 Segregation of duty should ensure that setting access rights in the access control system is separated from producing and issuing badges.

140 The access control system shall provide full traceability. All access attempts shall be logged, tailgating shall be effectively prevented, and unauthorized access attempts should be analyzed and associated action should be applied in case of incident.

Example:

In a typical setup, access to the building is controlled by electronic badge access.

Security areas (e.g. laboratory, data center, Security Control rooms) have dual authentication, e.g. badge with PIN or biometrics.

Tailgating is prevented by turnstiles, either full height turnstiles or guard monitored standard turnstile.

Access to high security areas (e.g. design, security lab) is controlled by automated mantraps with strong authentication.

141 In case physical keys are used to access the development area (i.e. where the key is the only access control measure) this area shall have a locking system independent from other areas. Such keys shall be kept secured in a safe place (e.g. key boxes, safe), with access only to authorized persons. Any withdrawal of a key shall be logged.

9.3.1.3 Securing offices, rooms and facilities

142 Physical security for offices, rooms, and facilities shall be designed and applied.

143 The development area should be alarmed and locked when unattended. Access controlled doors should be monitored with magnetic contacts and CCTV, and the restricted rooms should be monitored with motion detection.

9.3.1.4 Protecting against external and environmental threats

144 Appropriate physical protection against damage from fire, flood, and other forms of natural or man-made disaster should be designed and applied, preferably based on a risk assessment.

145 Access control and alarm system shall be protected to ensure proper function in case of natural or man-made disaster. This requirement also applies to logging and back-up systems.

9.3.1.5 Working in secure areas

146 Physical protection and guidelines for working in secure areas shall be designed and applied.

147 Personnel shall be aware that information may only be shared on a need-to-know basis.

148 People from external parties (e.g. customers, development partners, production partners, housekeeping, vendors, suppliers, carriers) shall not work in security areas without supervision of approved internals (e.g. host, owner of area, guard). This rule does not apply to externals who work as internal team members and are subject to the same security rules as internals

149 Vacant security areas shall be physically protected, e.g. with intrusion detection and fire alarm systems, and periodically checked.

150 Unauthorized use of photo and video cameras or audio recording equipment shall be prohibited.

9.3.1.6 Public access, delivery and loading areas

151 Access points such as delivery and loading areas, and other points where unauthorized persons may enter the premises shall be controlled and isolated from developer's processing facilities to avoid unauthorized access.

152 The design and layout of sites and premises should avoid high security areas next to public areas. The routes and walkways designated to visitors should be designed to ensure that visitors will not see restricted areas or information unintentionally.

Visitors

153 Visitors shall have only predefined, controlled access to the development environment. Procedures applying to visitors should include

- A documented application process for visits defining who is authorized to receive visitors and who is entitled to approve.
- A registration procedure ensuring that the visitor's identity is verified against an official government issued document (picture ID). Visitor information, the contact person in the development environment, time in and time out and the reason for the visit are recorded.

- Visitors display their visitor badge during the entire visit.
- Visitors are escorted at all times within the development environment either by a person from the development environment or by security personnel.

Delivery and shipment

154 Areas for incoming deliveries and outgoing shipments should be separated.

155 Delivery and shipping areas shall be designed such that no carrier personnel could gain access to other parts of the premises. External doors of these areas should be secured when internal doors are opened (interlock).

156 Carriers' drivers and trucks should be listed with name, photo, signature, make, license plate number. Only listed trucks and drivers may get access to the premises.

157 Deliveries to developer's premises should be announced. The carrier should not get access to developer's security areas, including shipping area and warehouse, but stay in delivery and loading area.

158 Delivery and loading area shall be monitored by CCTV. The recordings shall provide clear pictures enabling developer to identify any unintended unloading and loading.

159 Incoming material shall be registered on entry, and inspected for potential threats before delivery to the point of use.

9.3.1.7 Transportation

160 There are no particular requirements for physical transfer of materials within a physically secured area except that transfer shall be logged in order to provide full traceability.

161 The whole transport chain from initial development area to shipment of the TOE to the customer shall be controlled. Transport shall be monitored for security violations and any incidents shall be responded to and acted upon immediately.

162 The security measures during transit shall correspond to the confidentiality and integrity classification and should be defined in a written document.

163 At certain stages in the life cycle the TOE may be self-protecting according to CC part 1 line 136. In that case transportation security is not required.

Example:

During transportation, the TOE is attended at any time except while locked in an airplane.

Therefore the following rules apply to ground transportation

- packed in sealed transport boxes with unpredictable seal number (seal, plumb, or security tape)
- transport in a locked vehicle
- point-to-point transport without additional payload or hub/relation
- Two-man rule shall be applied during the entire transportation and the vehicle shall not be unattended at any time
- the transport should be equipped with mobile phone and GPS based surveillance

164 The TOE components shall be protected against tampering or theft during transit between physically separate secure areas. The protective mechanism shall enable the recipient to detect if tampering or theft has taken place.

165 A recipient should be provided with all information necessary to verify the integrity and authenticity of the shipment. The following information should be included.

- Number of boxes
- Seal number(s) of transport box(es)
- Number of pieces packed

166 Additionally, it may be useful to provide

- Route and schedule
- Drivers name, truck license plate number

167 In order to prevent attacks shipment information may be encrypted.

168 Upon receipt the recipient shall check the shipment without delay and acknowledge the integrity and authenticity status. In the event of a violation of shipment integrity or authenticity this acknowledgement shall be kept together with the original shipping notification.

9.3.2 Equipment security

169 *Objective:* To prevent loss, damage, theft, compromise, or loss of integrity of assets and security controls.

9.3.2.1 Equipment placing and protection

170 Security relevant equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

171 Equipment should be sited to minimize unnecessary access into work area and shall be positioned to minimize viewing angle from unauthorized persons during their use.

9.3.2.2 Supporting utilities

172 Security equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

173 All supporting utilities shall be adequate for the systems they are supporting and should be regularly inspected. The telecommunication equipment should be connected to the external provider by at least two diverse routes.

174 Power contingency plans should cover the measures to be taken on UPS (uninterruptible power supply) failure.

9.3.2.3 Cabling security

175 Power and telecommunications cabling carrying sensitive data or supporting security relevant information services shall be protected from interception or damage.

176 Network cabling should be protected from unauthorized interception or damage by avoiding routes through public areas.

177 For critical systems further controls shall be in place, e.g. line encryption and restricted access to switches and patch panels.

9.3.2.4 Equipment maintenance

178 Equipment should be correctly maintained to ensure its continued integrity and – for security systems - availability.

179 Where appropriate, classified information, data, and material shall be removed before maintenance.

180 Records of all suspected or actual faults should be kept, and appropriate controls should be implemented. All maintenance should be recorded with date, time, and personnel involved.

9.3.2.5 Security of equipment off-premises

181 Security measures should be applied to off-site equipment (Laptop, Mobile Phone, Handheld, Data carrier) taking into accounts the different risks of working outside the developer's premises. Utilization of such equipment shall be limited to activities not directly associated to the TOE and shall be authorized by management.

182 During business trips additional security measures (e.g. laptop in hand luggage, documents in safe) should be in place.

183 Classified information and data stored on a HDD of a mobile device shall be encrypted.

9.3.2.6 Secure disposal or re-use of equipment

184 All items of equipment containing storage media shall be checked to ensure that any sensitive data has been securely removed prior to disposal or re-use outside the developer’s premises.

185 Damaged devices, e.g. HDD which cannot be securely deleted shall be physically destroyed in a way that remains cannot be used in any meaningful way that might affect the confidentiality of the TOE or development assets, e.g. in a shredder.

9.3.2.7 Removal of property

186 Equipment, information or software shall not be taken off-site without prior authorization.

187 A procedure for the permission to take company properties off-site should be defined and deployed. Spot checks to detect unauthorized removal should be conducted in accordance with relevant legislations and regulations.

9.4 Communications and operations management

9.4.1 Operational procedures and responsibilities

188 *Objective:* To ensure the correct and secure operation of processing facilities.

189 Responsibilities and procedures for the management and operation of all processing facilities shall be established. This includes the development of appropriate operating procedures.

190 Segregation of duties should be implemented - where appropriate - to reduce the risk of negligent or deliberate system misuse.

9.4.1.1 Documented operating procedures

191 Operating procedures shall be documented, maintained, and made available to all users who need them.

192 Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, media handling, computer room and mail handling management, and safety.

193 The operating procedures should specify the instructions for the detailed execution of each job.

194 Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes should be authorized by management.

9.4.1.2 Change management

195 Changes to processing facilities and systems shall be controlled.

196 Operational systems and application software relevant for the development of the TOE or for security systems shall be subject to strict change management control.

197 In particular, the following items should be considered:

a) identification and recording of significant changes;

b) planning and testing of changes;

c) assessment of the potential impacts, including security impacts, of such changes;

d) formal approval procedure for proposed changes;

e) communication of change details to all relevant persons;

f) Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

198 Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information should be retained.

9.4.1.3 Segregation of duties

199 Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

200 Care shall be taken that no single person can

- access,
- modify, or
- use

assets without authorization or detection.

201 The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

202 Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

Example:
Network administration, server administration, and client administration are assigned to different IT departments. The respective log files are stored out of reach of the administrator. Access to the access control system is segregated from handling of physical badges, e.g. assigned to HR and security guards, respectively.

9.4.1.4 Separation of development, test and operational facilities

203 Development, test and operational facilities should be separated to reduce the risks to the confidentiality and integrity of the TOE. The level of separation between development, test, and operational environments that is necessary shall be identified and appropriate controls shall be defined and implemented.

9.4.2 Third party service delivery management

204 *Objective:* To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

205 The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team.

206 Where confidentiality and/or integrity of the TOE and its part is concerned Service Contracts and Statements of Works with external service providers and consultancy agencies shall pass the developer’s internal contract and vendor management responsible. The Security Manager shall be involved and any feedback considered.

207 Monitoring and review of third party services shall ensure that the security terms and conditions of the agreements are being adhered to, and that security incidents and problems are managed properly.

9.4.3 System planning and acceptance

208 *Objective:* To minimize the risk of systems failures for all systems supporting confidentiality and/or integrity of the TOE and its part.

9.4.3.1 Capacity management

209 The use of resources should be monitored and tuned to ensure the required system availability and performance.

210 Acceptance criteria for new processing systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. The Security Manager shall be involved and heard.

211 New processing systems, upgrades, and new versions should only be migrated into production after obtaining formal acceptance.

212 Appropriate tests should be carried out to confirm that all acceptance criteria have been fully satisfied. Acceptance may include a formal certification and accreditation process to verify that the security requirements have been properly addressed.

9.4.4 Protection against malicious and mobile code

213 *Objective:* To protect the integrity of software and information.

214 Virus, worms, Trojans, spyware and adware are considered malicious code based on the perceived intent of the author. Mobile code is software obtained from remote systems transferred across the network, e.g. java code, activeX controls, flash animations, office macros etc.

9.4.4.1 Controls against malicious code

215 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

216 For this purpose the following policies and rules should be considered:

a) A formal policy prohibiting the use of unauthorized software; Computers and all other equipment and materials provided by the developer shall be used for company purposes only. Downloading or storing unapproved software or data shall not be allowed.

b) Establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures have to be taken.

c) Conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated.

d) Installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis.

e) Defining management procedures and responsibilities to deal with malicious code protection on systems, including training in their use, alerting, reporting and recovering from malicious code attacks.

9.4.4.2 Controls against mobile code

217 Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from execution.

218 Access to mobile code on external web sites shall be restricted, e.g. on proxy servers. On the client, with the restricted/trusted sites mechanism of the browser, access to websites containing mobile code should only be granted after formal approval.

9.4.5 Back-up

219 *Objective:* To maintain the integrity and availability of information and information processing facilities related to the TOE and security systems, without disclosure where confidentiality is required.

220 Backups shall be created, stored and destroyed according to a procedure approved by the Security Manager. This procedure shall ensure that the level of security applied to back-ups is the same as for the original data.

221 Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure while maintaining confidentiality and integrity of the TOE and its part. Beside all information and data related to the TOE, e.g. design data and CM system, access control and administrator log files shall be backed-up.

222 The retention period for essential information and any requirement for archiving information permanently should be determined.

223 Back-up arrangements should be regularly tested to ensure that they meet the requirements of the agreed backup policy. For critical systems, the backup arrangements should cover all system information, applications, and data necessary to recover all TOE related and security systems in the event of a disaster.

9.4.6 Network security management

224 *Objective:* To ensure protection of information in networks and protection of the supporting infrastructure.

225 Only authorized people shall have access to electronic information and data related to the TOE.

226 The entry point into the development area's network shall be protected at the network boundary by a mechanism that restricts network traffic to a minimum, defined in a policy.

227 Regulations for the segregation of network segments depending on their security categorization shall be defined. Networks for development activities shall be separated from networks for other (e.g. office) applications either physically or by VLAN technologies, protected by access control measures and appropriate firewall rules.

228 Where confidentiality is a requirement, access to development networks should only be possible with Thin Clients (terminals) or hardened clients which effectively prevent copying network content (e.g. no I/O except monitor, keyboard, and mouse). Development networks shall not have wireless connectivity.

229 The necessary hardware (e.g. server, firewall, router, patch panel etc.) and administration shall be located in properly secured premises consistent with the security level of the development area.

9.4.6.1 Network controls

230 Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

231 Where confidentiality and/or integrity are requirements, developer shall implement controls to ensure security of information in networks, and protection of connected services from unauthorized access. In particular, the following items should be considered:

a) Operational responsibility for networks separated from computer operations, e.g. network operation center for administration of network devices and local administration of servers;

b) Special controls to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications; special controls to maintain the availability of the network services and computers connected as far as security systems are concerned

c) Appropriate logging and monitoring to enable recording of security relevant actions;

d) Management activities coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the processing infrastructure.

232 It should not be possible to view and/or modify configuration items from outside the defined development area, even from within the corporate network. A strong authentication scheme shall be defined for network access.

233 The development machines shall be configured with a controlled, restrictive user security policy that prevents the installation of additional unauthorized functionality. Members of the development environment should not have administrator rights to the IT systems which they work with.

234 A mechanism shall be employed between the corporate/public network boundary and the development area IT systems that provides up-to-date commercial grade protection against logical attacks.

Example:
In a typical setup the network is protected with

- Application layer firewalls with restrictive rules
- Network admission control
- Intrusion detection/prevention systems
- Virus/malware protection

9.4.6.2 Security of network services

235 Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or are outsourced.

236 The developer should segregate duties in IT administration (network, server, client, application administration). Administrator log files should be kept secured out of reach of the administrator.

9.4.7 Media handling

237 *Objective:* To prevent unauthorized disclosure, modification, removal or destruction of TOE related information, data and material.

238 Classified data (confidential or strictly confidential) shall be encrypted while stored on movable data carrier and during transit.

239 Media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, HDD, USB Sticks, CD/DVD/BD), mobile devices (smartphones), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

9.4.7.1 Management of removable media

240 Where confidentiality and/or integrity are required, procedures shall be in place for the management of removable media. The following guidelines for the management of removable media should be considered:

a) permission of removable media drives only if need is evident;

b) all media stored in a safe, or secure environment, in accordance with developer's specifications;

c) where necessary and practical, for media a removal authorization process and a record of such removals kept in order to maintain an audit trail;

d) registration of removable media to limit the opportunity for data loss.

241 All procedures and authorization levels should be clearly documented.

9.4.7.2 Disposal of media

242 Media shall be disposed of securely and safely when no longer required, using formal procedures.

243 Formal procedures for the secure disposal of media should minimize the risk of sensitive information leakage to unauthorized persons. The procedures for secure disposal of media containing sensitive information should be commensurate with the sensitivity of that information.

244 The following items may be considered:

a) media containing sensitive information should be stored and disposed securely, e.g. by shredding and incineration, or sanitizing for further use within the organization;

b) careful selection of service providers for the collection and disposal services for papers, equipment and media; only suitable contractors with adequate controls, experience, and reputation should be contracted;

c) witness disposal of sensitive items by trustworthy developer's employees and log as appropriate in order to maintain an audit trail.

245 When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of non-sensitive information to become sensitive.

9.4.8 Exchange of information

246 Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

247 Exchanges of information and software between organizations should be based on a formal exchange policy, carried out in line with exchange agreements.

248 Procedures and standards should be established to protect information and physical media containing information in transit.

9.4.8.1 Information exchange policies and procedures

249 Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

250 Data transfer to/from secured networks should only be possible via drop box mechanism with restricted access to DMZ accounts. Where confidentiality and integrity of the TOE and its parts is required, transfer of related information and data shall be encrypted and signed. If only integrity of the TOE and its parts is required, transfer of related information and data shall be signed.

9.4.8.2 Exchange agreements

251 Agreements should be established for the exchange of information and software between the organization and external parties.

252 Policies, procedures, and standards should be established and maintained to protect information and physical media in transit, and should be referenced in such exchange

agreements. The security content of any agreement should reflect the sensitivity of the business information involved.

9.4.8.3 Physical media in transit

253 Where confidentiality and/or integrity are requirements media containing classified information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

254 The following guidelines should be considered to protect information media being transported between sites:

a) use only company approved couriers;

b) adopt controls, where necessary, to protect sensitive information from unauthorized disclosure or modification; examples include:

1. use of locked containers;
2. delivery by hand;
3. tamper-evident packaging (which reveals any attempt to gain access);
4. in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

9.4.8.4 Electronic messaging

255 Information involved in electronic messaging shall be appropriately protected. Security considerations for electronic messaging should include the following:

a) Protecting messages from unauthorized access (password, encryption) or modification;

b) ensuring correct addressing and transportation of the message;

c) ensuring authenticity of the message, i.e. sender/author of the message should be unambiguous;

d) strong authentication restricting access from publicly accessible networks, e.g. client certificate and VPN.

Rules should be available for the usage of email systems for users and for persons in charge of the email system, particularly dealing with

a) spam or malware filter on the gateway and mail server levels

b) responsibility for distribution lists.

9.4.9 Electronic commerce services

256 Objective*:* To ensure the security of electronic commerce services, and their secure use.

257 Not applicable

9.4.10 Monitoring

258 Objective: To detect unauthorized processing activities.

9.4.10.1 Audit logging

259 Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period (e.g. three months online, one year offline as required by payment schemes) to assist in future investigations and access control monitoring.

260 Logging facilities and log information shall be protected against tampering and unauthorized access.

9.4.10.2 Administrator and operator logs

261 System administrator and system operator activities shall be logged. These log files should be kept out of reach of the respective administrator or system operator, respectively, and checked at least monthly for suspicious activities.

9.4.10.3 Fault logging

262 All clients shall use the Security Event log function to be able to trace unwanted login attempts or security breaches. Network related systems like domain controllers, firewalls, or proxy servers shall have logging enabled.

9.5 Access control to information systems

9.5.1 Business requirement for access control

263 Objective: To control access to information.

264 Access to information, information processing facilities, and business processes shall be controlled on the basis of security requirements.

9.5.1.1 Access control policy

265 An access control policy shall be established, documented, and reviewed based on security requirements for access.

266 Access control rules and rights for each user or group of users shall be clearly stated in an access control policy. Access controls are both logical and physical. Users and service providers shall be given a clear statement of the business requirements to be met by access controls.

267 Access shall be granted only on a need-to-know basis.

268 The policy should take into account

a) security requirements of developers business activities;

b) policies for information dissemination and authorization, e.g. the need-to-know principle and security levels and classification of information;

c) consistency between the access control and information classification policies of different systems and networks;

d) relevant legislation and any contractual obligations regarding protection of access to data or services;

e) management of access rights in a distributed and networked environment which recognizes all types of connections available;

f) segregation of access control roles, e.g. access request, access authorization (manager, system and/or data owner, project manager), access administration (IT coordinator, system administrator, Helpdesk) for both, access to premises and access to systems.

9.5.2 User access management

269 Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

270 The procedures shall cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer need access to information systems and services. Special attention shall be given to the need to control the allocation of privileged access rights.

9.5.2.1 User registration

271 There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

272 The access control procedure for user registration and de-registration should include:

a) using unique user IDs (e.g. user accounts) to enable users to be linked to and held responsible for their actions; the use of group IDs shall only be permitted where they are necessary for business or operational reasons, and shall be approved and documented; responsible persons for such group IDs shall be named.

b) checking that the user has authorization from the system owner for the use of the information system or service; separate approval for access rights from management may also be appropriate;

c) checking that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy, e.g. it does not compromise segregation of duties;

d) giving users a written statement of their access rights;

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring service providers do not provide access until authorization procedures have been completed;

g) maintaining a formal record of all persons registered to use the service, e.g. Active Directory;

h) immediately removing or blocking access rights of users who have changed roles or jobs, or left the organization;

i) periodically checking for, and removing or blocking, redundant user IDs and accounts;

j) ensuring that user IDs are not re-issued to other users.

273 Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or service agents.

9.5.2.2 Privilege management

274 The allocation and use of privileges shall be restricted and controlled.

275 Multi-user systems that require protection against unauthorized access shall have the allocation of privileges controlled through a formal authorization process.

276 The following steps shall be considered:

a) the access privileges associated with each system, e.g. operating system, database management system and each application, and the users to which they need to be allocated shall be identified;

b) privileges shall be allocated to users on a need-to-use basis

c) an authorization process and a record of all privileges allocated shall be maintained. Privileges shall not be granted until the authorization process is complete;

d) the development and use of system routines should be promoted to avoid the need to grant privileges to users;

e) the development and use of programs which avoid the need to run with privileges should be promoted.

277 Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems.

9.5.2.3 User password management

278 The allocation of passwords shall be controlled through a formal management process.

279 The process shall consider the following requirements:

a) users should be required to sign a statement to keep personal passwords confidential; this signed statement could be included in the terms and conditions of employment;

b) when users are required to maintain their own passwords they should be provided initially with a secure temporary password, which they are forced to change immediately;

c) establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;

d) temporary passwords shall be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages shall be avoided;

e) temporary passwords shall be unique to an individual and shall not be guessable;

f) passwords shall never be stored on computer systems in an unprotected form;

g) default vendor passwords shall be altered following installation of systems or software.

280 Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Other technologies for user identification and authentication, such as biometrics, e.g. finger-print verification, signature verification, and use of hardware tokens, e.g. smart cards, are available, and should be considered - where appropriate – to replace password.

9.5.2.4 Review of user access rights

281 Management shall review users' access rights at regular intervals using a formal process.

282 The review of access rights shall consider the following guidelines:

a) users' access rights should be reviewed at regular intervals, e.g. a period of 6 months

b) users' access rights should be reviewed after any changes, such as promotion, demotion, or termination of employment;

c) privilege allocations shall be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

d) changes to privileged accounts shall be logged for periodic review.

283 It is necessary to regularly review users' access rights to maintain effective control over access to data and information services.

9.5.3 User responsibilities

284 Objective: To prevent unauthorized user access, and compromise of confidentiality and integrity of the TOE or its parts.

285 The co-operation of authorized users is essential for effective security. Users shall be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

9.5.3.1 Password use

286 Users shall be required to follow good security practices in the selection and use of passwords.

287 In the Password Policy all users shall be required to:

a) keep passwords confidential;

b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved, e.g. a password safe;

c) change passwords whenever there is any indication of possible system or password compromise;

d) select quality passwords with sufficient minimum length (at least 8 characters), e.g. at least one character from 3 out of the following 4 categories:

- Lower case characters (a...z)
- Upper case characters (A...Z)
- Numerical characters (0...9)
- Special characters (!"$%&/()=?*....);

e) change passwords at regular intervals, e.g. every 90 days;

f) change temporary passwords at the first log-on;

g) do not include passwords in any automated log-on process, e.g. stored in a macro or function key;

h) do not share individual user passwords;

i) do not use the same password for business and non-business purposes.

9.5.3.2 Unattended user equipment

288 Users shall ensure that unattended equipment has appropriate protection.

289 Where relevant, all users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

290 Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

b) log-off mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);

c) secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access (CTRL-ALT-DEL in Windows), when not in use;

d) movable equipment (notebook) should be secured (e.g. with cable lock Kensington lock) or kept in a locked cabinet when not in use;

e) data media should be kept locked unless encrypted.

291 Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period.

9.5.3.3 Clear desk and clear screen policy

292 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted to reduce the risk of a security breach, fraud, and information theft facilitated by unattended documents or media.

293 The clear desk and clear screen policies should provide guidance to all users regarding handling of documents, data, and media according with respect to their classification (see 9.1.2).

9.5.4 Network access control

294 Objective: To prevent unauthorized access to networked services.

295 It shall be ensured that user access to networks and network services can not compromise the security of the network services by:

a) appropriate interfaces between the organization's network and networks owned by other organizations, and public networks;

b) appropriate authentication mechanisms for users and equipment;

c) control of user access to information services.

Example:

Cascading networks ensures that access to a network is granted from an appropriate security level. Connected clients are member of the respective Windows Client Domain and can be identified via certificates.

For high security networks MAC-address-filtering and patched connections are deployed.

296 Firewall Syslog messages should be analyzed regularly and actions are taken when necessary.

9.5.4.1 Policy on use of network services

297 Users shall only be provided with access to the services that they have been specifically authorized to use.

9.5.4.2 User authentication for external connections

298 Where remote access to developers' networks is permitted appropriate authentication methods shall be used to control access by remote users. Where confidentiality is required, remote access to security networks, particularly networks where TOE or its parts or related design information is handled, shall not be possible.

299 Where only integrity is required remote access may be allowed with suitable security measures ensuring integrity and the same level of network security as in the developer's premises.

300 Remote users shall get access to the developer's network based on strong authentication only.

9.5.4.3 Equipment identification in networks

301 Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

302 Equipment identification should be used if it is important that the communication can only be initiated from a specific location or equipment. An identifier in or attached to the equipment (certificate, MAC address) can be used to indicate whether this equipment is permitted to connect to the network. These identifiers should clearly indicate to which network the equipment is permitted to connect, if more than one network exists and particularly if these networks are of differing sensitivity. It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

303 This control can be complemented with other techniques to authenticate the equipment's user. Equipment identification shall only be applied in addition to user authentication.

Example:

Employees and business partners with notebooks installed and managed by developer's IT (machine certificates) are enabled to get full network access to developer's intranet, file server, and Exchange Server (but not to the development network!) while business partners and contractors without developer's equipment get only restricted access to some applications hoste in the DMZ.

9.5.4.4 Remote diagnostic and configuration port protection

304 Physical and logical access to diagnostic and configuration ports shall be controlled.

305 Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port. An example for such a supporting procedure is to ensure that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

306 Ports, services, and similar facilities installed on a computer or network facility which is not specifically required for business functionality should be disabled or removed.

9.5.4.5 Segregation in networks

307 Groups of information systems, information services, or users should be segregated on networks, e.g. in different security zones or network branches.

308 Where confidentiality and/or integrity are requirements, the following high-level requirements shall apply to all security zones or network branches of all levels.

a) The interconnection of distributed parts of a security zone or network branch shall be encapsulated / protected by the use of secure network techniques, e.g. VPN.
The term secure VPN is used for VPNs without potential eavesdropping risk,

e.g. by the use of IPSec or SSL encrypted tunnels or special physically secured in-house links if another security zone is crossed;

b) All interconnections between security zones and network branches shall be planned and controlled by a central authority, involving the Security Manager;

c) Responsibility for the interconnections and for the data processed within the security zones themselves should be segregated to deploy four-eye principle (This means that it shall not be possible for a single person to establish a data channel outbound or inbound).

9.5.4.6 Network connection control

309 For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control regulations and requirements of the business applications.

310 The network access rights of users shall be maintained and updated as required by access control regulations.

311 The connection capability of users can be restricted through network gateways that filter traffic, e.g. by means of pre-defined tables or rules (application layer firewall).

312 Dedicated processes and guidelines for business partner access and interconnections with/to business partners shall be defined and documented. All network connection requests shall be documented.

9.5.4.7 Network routing control

313 Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

314 Routing controls shall be based on positive source and destination address checking mechanisms. Security gateways should utilize at least either

a) firewalls to validate source and destination addresses on the network layer;

b) proxy server to validate source and destination addresses on application layer;

c) SOCKS proxy server for user authentication.

315 Shared networks, especially those extending across organizational boundaries, may require additional routing controls. This particularly applies where networks are shared with third party (non-organization) users.

9.5.5 Operating system access control

316 Objective: To prevent unauthorized access to operating systems.

317 Security facilities shall be used to restrict access to operating systems to authorized users. The facilities should be capable of the following:

a) authenticating authorized users, in accordance with a defined access control policy;

b) recording successful and failed system authentication attempts;

c) recording the use of special system privileges;

d) issuing alarms when system security policies are breached.

9.5.5.1 Secure log-on procedures

318 Access to operating systems shall be controlled by a secure log-on procedure.

319 The procedure for logging on to an operating system shall be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance.

9.5.5.2 User identification and authentication

320 All users shall have a unique identifier for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

321 This is mandatory for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators).

322 Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

323 New user accounts shall be requested via a defined process in order to make sure that user accounts will be created, revoked or deleted according to the account policies, and follow the defined naming conventions.

9.5.5.3 Password management system

324 Systems for managing passwords shall be interactive and ensure quality passwords.

325 The password management system shall enforce and support the password requirements as defined in 9.5.3.1. Additionally, the password managing system shall

a) store password files separately from application system data;

b) store and transmit passwords in protected (e.g. encrypted or hashed) form.

9.5.5.4 Use of system utilities

326 The use of utility programs that might be capable of overriding system and application controls shall be restricted on a need-to basis and tightly controlled.

9.5.5.5 Session time-out

327 Inactive sessions should shut down after a defined period of inactivity.

328 A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. The time-out delay should reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment.

329 A limited form of time-out facility is the password protected screensaver which is part of the Windows installation. It clears the screen and prevents unauthorized access but does not close down the application or network sessions.

9.5.5.6 Limitation of connection time

330 Connection time controls should be considered for sensitive computer applications, e.g. those with access to the TOE and its parts in order to provide additional security for high-risk networks or applications.

9.5.6 Application and information access control

331 Objective: To prevent unauthorized access to information held in application systems.

9.5.6.1 Information access restriction

332 Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policies.

333 Need-to-know principle shall be implemented throughout the entire application landscape, e.g. project specific access rights, restricted access to work shares.

9.5.6.2 Sensitive system isolation

334 Sensitive systems shall have a dedicated (isolated) computing environment.

335 Sensitive application systems (e.g. development networks, IT Administration Network) shall not run in shared environments. The necessary shared services (e.g. Active Directory, Netinstall, license server, drop box) shall be installed in a DMZ. Data should be transferred via drop box mechanisms.

9.5.7 Mobile computing and teleworking

336 Objective: To ensure information security when using mobile computing and teleworking facilities.

337 Where confidentiality is required, mobile computing of the TOE or its parts or related design information shall not be possible.

338 Teleworking with access to the TOE or its parts or related design information shall only be allowed if confidentiality is not required. The teleworking environment (premises, IT etc.) shall meet all requirements related to integrity set in this document. If teleworking is permitted processes shall be in place to ensure integrity during all teleworking activities.

9.5.7.1 Mobile computing and communications

339 A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing (laptop, handheld devices) and communication facilities (smart phones etc.).

340 Care should be taken when using mobile computing facilities in public places (even inside the premises), meeting rooms and other unprotected areas outside of the organization’s premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.

9.5.7.2 Teleworking

341 A policy, operational plans and procedures shall be developed and implemented for teleworking activities if applicable.

342 Teleworking uses communications technology to enable staff to work remotely from a fixed location outside of their organization. Suitable protection of the teleworking site requires the same security implementation as in the office workplace.

9.6 Information systems acquisition, development and maintenance

343 Information systems include operating systems, infrastructure, business applications, services, off-the-shelf products, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security.

9.6.1 Security requirements of information systems (informative)

344 Objective: To ensure that security is an integral part of information systems.

345 Security requirements shall be identified and agreed upon prior to the development and/or implementation of information systems.

346 All security requirements shall be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

347 The development of Application has to follow the rules for application development and software distribution.

9.6.1.1 Security requirements analysis and specification (informative)

348 Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

349 When products are purchased, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement the risk introduced and associated controls should be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this functionality should be disabled or the proposed control structure should be reviewed.

9.6.2 Correct processing in applications

350 Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications, ensuring confidentiality and/or integrity of the TOE and its parts.

351 Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

352 Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

9.6.2.1 Input data validation (informative)

353 Data input to applications with impact on security and/or integrity of the TOE and its parts shall be validated to ensure that this data is correct and appropriate.

354 Checks should be applied to the input of data. The following guidelines should be considered:

a) dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect errors;

b) periodic review of the content of key fields or data files to confirm their validity and integrity;

c) inspecting hard-copy input documents for any unauthorized changes (all changes to input documents should be authorized);

d) procedures for responding to validation errors;

e) procedures for testing the plausibility of the input data;

f) defining the responsibilities of all personnel involved in the data input process;

g) creating a log of the activities involved in the data input process.

355 Automatic examination and validation of input data should be considered, where applicable, to reduce the risk of errors and to prevent attacks.

9.6.2.2 Control of internal processing

356 The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimized. Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate. Specific areas to consider include:

a) the use of add, modify, and delete functions to implement changes to data;

b) the procedures to prevent programs running in the wrong order or running after failure of prior processing;

c) the use of appropriate programs to recover from failures to ensure the correct processing of data;

d) protection against attacks.

9.6.2.3 Message integrity (informative)

357 An assessment of security risks should be carried out to determine if message integrity is required and to identify the most appropriate method of implementation.

358 The integrity of electronic mail communication should be ensured by using the encryption and signing functionality based on PGP-Keys or S/MIME certificates.

9.6.2.4 Output data validation (informative)

359 Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

360 Output validation may include:

a) plausibility checks to test whether the output data is reasonable;

b) reconciliation control counts to ensure processing of all data;

c) providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;

d) procedures for responding to output validation tests;

e) defining the responsibilities of all personnel involved in the data output process;

f) creating a log of activities in the data output validation process.

361 Typically, systems and applications are constructed on the assumption that having undertaken appropriate validation, verification, and testing, the output will always be correct. However, this assumption is not always valid; i.e. systems that have been tested may still produce incorrect output under some circumstances.

9.6.3 Cryptographic controls

362 Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

9.6.3.1 Policy on the use of cryptographic controls

363 A policy on the use of cryptographic controls for protecting information shall be developed and implemented.

364 Cryptographic controls can be used to achieve different security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b) integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;

c) non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

365 Encryption keys shall be based on open algorithms and a key shall be derived from a random with sufficient entropy to prevent brute force attacks (e.g., in 2012 German BSI requires at least 80 bits of entropy, i.e. 256 bit symmetric or 2048 bit asymmetric RSA key length).

9.6.3.2 Key management

366 Key management shall be in place to support the organization's use of cryptographic techniques.

367 All cryptographic keys shall be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys shall be physically protected.

368 The key management processes should include

a) generating keys

b) generating and obtaining public key certificates;

c) distributing keys to intended users, including how keys are activated when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;

g) revoking keys;

h) recovering keys;

i) archiving keys, e.g. for information archived or backed up;

j) destroying keys;

k) logging and auditing of key management related activities.

9.6.4 Security of system files

369 Objective: To ensure the security of system files.

9.6.4.1 Control of operational software

370 There shall be procedures in place to control the installation of software on operational systems.

371 To minimize the risk of corruption to operational systems, the following guidelines should be considered to control changes:

a) updating of the operational software, applications, and program libraries is performed by IT administrators upon IT internal processes.

b) Users are not allowed to install software which is not approved by the developer.

c) The process to add new software should include defined testing and release scenarios.

d) Patches and updates should be provided in a timely manner. In production environments service windows should be defined to allow updates to highly available systems.

372 Any decision to upgrade to a new release should take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version.

373 Physical or logical access shall only be given to suppliers for support purposes when necessary. The supplier's activities shall be monitored.

374 Computer software may rely on externally supplied software and modules, which shall be monitored and controlled to avoid unauthorized changes which could introduce security weaknesses.

9.6.4.2 Protection of system test data

375 Test data shall be carefully selected, protected and controlled.

376 The use of operational databases containing sensitive information for testing purposes should be avoided. If sensitive information systems have to be used for testing purposes, all sensitive details and content should be removed or modified beyond recognition before use.

9.6.4.3 Access control to program source code

377 Objective: Restricted access to program source code.

378 Access to program source code and associated items (such as development tools, test cases, etc.) should be strictly controlled in order to maintain integrity of the TOE.

379 The TOE and its parts are controlled by a CM system (see 9.1.1.3).

9.6.5 Security in development and support processes

380 Objective: To maintain the security of application system software and information.

9.6.5.1 Change control procedures

381 Change control procedures shall be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control, and managed implementation.

382 This process should include a risk assessment, analysis of the impact of changes, and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

9.6.5.2 Technical review of applications after operating system changes

383 When operating systems or applications are changed, critical applications shall be monitored to ensure there is no adverse impact on security.

384 Responsibility for monitoring vulnerabilities and vendors releases of patches and fixes shall be assigned.

9.6.5.3 Restrictions on changes to software packages

385 Modifications to software packages with impact on the TOE and its parts (e.g. development tools, test cases) should be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

386 As far as possible, and practicable, vendor-supplied software packages should be used without modification. If changes are necessary the original software should be retained

and the changes applied to a clearly identified copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades.

9.6.5.4 Information leakage

387 Where confidentiality is required opportunities for information leakage should be prevented.

Example:

In a typical high security area the outbound data transmission is restricted to defined people and logged. Where utilization of mobile data media, e.g. USB-Devices, is inevitable, it is restricted to persons with approved privileges, e.g. by means of port protector tools. Data is encrypted before leaving a secure network.

9.6.5.5 Outsourced software development (informative)

388 Outsourced software development shall be supervised and monitored by the developer, e.g. by using secure development lifecycle procedures.

389 Where software development is outsourced, the following points should be considered:

a) licensing arrangements, code ownership, and intellectual property rights;

b) escrow arrangements in the event of failure of the third party;

c) contractual requirements for quality and security functionality of code;

d) testing before installation to detect malicious code.

9.6.6 Technical Vulnerability Management (informative)

390 Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

391 There are two main different threads: published technical vulnerabilities of purchased software and systems, and self developed systems with improper implementation of security measures.

9.6.6.1 Control of technical vulnerabilities (informative)

392 Timely information about technical vulnerabilities of information systems being used shall be obtained, the developer's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

393 Where confidentiality and/or integrity are requirements, security shall be integral part of software and system development projects.

9.7 Information security incident management

9.7.1 Reporting information security events and weaknesses

394 Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

395 All security related incidents and weaknesses shall be reported to the Security Manager.

9.7.1.1 Reporting information security events

396 Information security events shall be reported through appropriate management channels as quickly as possible.

397 A rule providing suitable feedback processes to ensure timely information about security incidents should be in place. In particular, minimum criteria for reporting an event should be defined.

9.7.1.2 Reporting security weaknesses

398 All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

399 The report shall be addressed to the Security Manager, where possible with evidence. Depending on the context it may be necessary to react immediately or wait Security Manager decision for action.

9.7.2 Management of information security incidents and improvements

400 Objective: Effective management of information security incidents ensures appropriate level of security.

9.7.2.1 Responsibilities and procedures

401 Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to security incidents.

402 All security incidents shall be reported immediately to the Security Manager. Beside immediate containment all responses to security incidents shall be agreed upon with the Security Manager.

403 Security incident should be documented in an access controlled, secured environment.

9.7.2.2 Learning from information security incidents (informative)

404 There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

405 Information security incidents shall be analyzed, corrective and preventive actions derived and results reported in the regular security report.

9.7.2.3 Collection of evidence (informative)

406 Where a follow-up action against a person or organization after an security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdictions (e.g. code of criminal procedure, privacy legislation, workers council involvement).

9.8 Business continuity management

9.8.1 Security aspects of business continuity management

407 Objective: To counteract interruptions to systems necessary to maintain the required level of security and/or integrity and to ensure their timely resumption.

9.8.1.1 Including security in the business continuity management process

408 The security environment for the TOE and its parts should be maintained in case of incidents, accidents, and crisis situations. Therefore, a managed process should be developed and maintained for business continuity throughout the organization that addresses the security requirements.

409 In terms of IT and information security the process should address network protection, computer centers incl. hardware, access control systems, and monitoring and alarm systems.

9.8.1.2 Business continuity and risk assessment (informative)

410 Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for the TOE or its parts.

411 The developer is responsible for business continuity planning in his respective business within the framework of his entrepreneurial responsibility. All existing design, production, logistics and supply chain systems, structures and processes shall plan for sufficient contingency to appropriately mitigate the effects of disasters, business interruptions and/or risks as identified in accordance with risk assessment procedures.

9.8.1.3 Developing and implementing continuity plans including security (informative)

412 Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, security relevant processes.

413 In particular, attention shall be put on the protection of the TOE in case of an incident. This may include, but is not limited to

a) Automated shut down of IT systems;

b) Automatically closing emergency exits;

c) Deployment of additional security staff.

9.8.1.4 Business continuity planning framework (informative)

414 A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address security requirements, and to identify priorities for testing and maintenance.

9.8.1.5 Testing, maintaining and re-assessing business continuity plans (informative)

415 Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

9.9 Compliance (informative)

416 Objective: To avoid breaches of any statutory, regulatory or contractual obligations related to the TOE.

417 Although compliance is not a CC requirement a lack of compliance can impair the TOE and its parts. Therefore it may be necessary to identify relevant legislation, statutory, regulatory and contractual requirements, third party intellectual property rights, and other applicable regulations.