Joint Interpretation Library

Minimum Site Security Requirements

Version 2.1 (for trial use)

December 2017

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.

1.1.1 Harmonization

2 The Common Evaluation Methodology (CEM) 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. 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).

3 The requirements set in this document are "minimum" in the sense that

- All developers have to implement the controls and related security measures defined in this document
- Additional requirements could apply to facilitate the ST, or to meet the protection needs of the TOE.

1.1.2 Clarification on "other deliverables" (site audit scope)

4 According to ALC_DVS the evaluator may need to examine input from ALC_CMS.4 and ALC_CMC.4 to determine that the security controls are well-defined and followed.

5 According to CEM some work units of ALC_CMC, ALC_CMS, ALC_DEL and ALC_TAT require that documentary evidence should be supplemented by visiting the development environment in order to check the evidence that the procedures are being applied.

6 MSSR with its defined security objectives and described security measures focus on ALC_DVS; it may have links to and interdependencies with other work units but does not set requirements for them.

7 This document covers the controls that shall be considered for the development environment to have the appropriate level of protection to maintain confidentiality and integrity of the TOE corresponding to the overall attack potential AVA_VAN.5 claimed for the TOE. The specified objectives are consistent and mutually supportive.

1.2 Structure of Chapters and Controls

8 This document defines the necessary security measures based on an independent, collective analysis, and a shared experience of best practices from developers, evaluators, and certification bodies organized in ISCI working group.

9 Every chapter 9.1 through 9.8 consists of one or more security controls. All controls have to be considered by the developer but may be omitted with justification if not applicable.

10 In this document, chapter 9.1 “Asset Management” defines the assets to be protected, the necessary policies, and their content in order to be compliant with CEM.

11 Chapters 9.2 to 9.8 of this document detail the security controls with objectives and describes the security measures that are necessary to protect the assets related to the TOE.

12 All Controls have of two level of requirements, objectives and measures, the latter structured in Policies and Security Measures

13 Each Control is structured into 3 chapters:

- Objective - defines the mandatory target of the control, i.e. what shall be achieved by the respective security measures. As long as a control is applicable the objectives cannot be omitted.
- Policies - defines the policies mandatory to facilitate the objective
- Security Measures - describes the expected security measures (see 1.3.1) that are necessary to protect the assets related to the TOE. Security measures shall be modified, replaced, or omitted only with justification, providing clear evidence that the required level of security is achieved.

In some controls, a fourth chapter is added in order to facilitate elucidation:

- Examples - illustrate requirements with typical set-up or implementation, where appropriate. These examples are for explanation purpose and do not have to be systematically implemented as is.

14 In the Exhibit typical implementations are described for common types of sites.

15 The controls and control objectives described in this document are not exhaustive; additional control objectives and controls may also be selected, where necessary.

1.3 Application

16 The current document status is "trial use" for Common Criteria evaluation of Smartcard and similar devices (SC&SD), including related software development. Related software comprises SW necessary to operate the SC&SD (FW, OS), SW which contributes to the security of SC&SD, and SW running on the SC&SD.

17 This document is currently also guidance for site security certification of sites claiming compliance with CC security requirements.

18 The document is based on CEM paragraphs 1102ff. and CEM Annex A.4.3.2. The requirements are structured according to ISO27001:2013. An information security management system certified according to ISO27001 is neither necessary nor sufficient to pass Common Criteria evaluation.

19 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.

20 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.

21 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.

1.3.1 Developer

22 In order to fulfill the CC work units for ALC_DVS the developer shall achieve all applicable objectives set in this document. Therefore, appropriate measures, typically as described in the sub-chapters Security Measures, shall be implemented in a meaningful and concerted way.

23 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 needs derived from the ST and the objectives defined in this document.

24 If developer implements a different security setup, e.g. modified, replaced, or omitted security measures, developer has to ensure and to demonstrate that the objectives are fulfilled and the required level of security is achieved. Developer shall provide justification to the evaluator.

25 The developer can refer to this document in order to support justification that the measures maintain confidentiality and integrity.

1.3.2 Evaluation Body (ITSEF)

26 Consistently with §13.5 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.

27 ALC_DVS targets all the sites at which TOE development occurs and that are identified in the development security documentation. This document must be used for the assessment of each of these sites.

28 ALC_DVS.1.1 and ALC_DVS.2.1 specify that the evaluator shall examine the development security documentation to determine that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation.

29 In order to determine the sufficiency of the security measures employed the ITSEF shall examine

- the development confidentiality and integrity policies and assumptions of the ST ,
- the justification (e.g. risk assessment) for any exclusion or incomplete implementation of controls, and

- the correct and concerted implementation of the measures required in the controls.

30 If the ST identifies security objective(s) for the development environment that call for specific requirements for the policies, the evaluator shall take it into account for the assessment.

31 ALC_DVS.2.2 specifies that the evaluator shall examine the development security documentation to determine that an appropriate justification is given why the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

32 The evaluator shall examine the correct and concerted implementation of the measures required in the controls. If developer implements the controls incompletely or with different security measures than the expected ones the justification provided by the developer should include a demonstration that the required level of security is achieved.

33 The evaluator shall examine this demonstration and determine whether or not the objectives defined in chapter 9 of this document are achieved.

34 The evaluator shall determine that the justification takes into consideration the ST for any information that may give rise to additional requirements for the development environment security.

35 The evaluator shall determine that the justification covers all aspects of development and production on all the different sites with all roles involved up to delivery of the TOE and that the application of this document to these different stages and sites is done correctly and consistently.

36 The requirements defined in this document should be used by the evaluator to create a checklist to prepare the site visit and the examination of evidence that are required by ALC_DVS.1.3 and ALC_DVS.2.4.

2 Normative references

37 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, April 2017, Version 3.1 Revision 5
- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1 Revision 5
- ISO/IEC 27002:2013, Information technology - Security techniques - Code of practice for information security management

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

- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements
- ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management

3 Terms and Definitions

39 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 and data provided to produce the TOE
Availability	The property of being accessible and usable upon demand by an authorized entity
Business operations	General term for the entirety of operations performed by the developer related to the TOE, e.g. “personalization” is part of business operations
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation, Part 1-3, April 2017, Version 3.1, Revision 5
COBIT	Control Objectives for Information and Related Technology
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Control	Set of measures, associated to one or more objectives, intended to respond to threats
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 Documentation
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
FW	Firmware
High Security Area	Area where TOE related data or material classified “critical” or “very critical” is accessible, and Security Control areas (access control and intrusion detection) where applicable
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
ITIL	Information Technology Infrastructure Library
ITSEF	Information Technology Security Evaluation Facility; Evaluation Body
Malicious code	Virus, worms, Trojans, spyware and adware based on the perceived intent of the author.
Mobile code	Software obtained from remote systems transferred across the network, e.g. Java code, activeX controls, flash animations, office macros etc.
Mobile Computing	Data processing on a mobile device, either online or offline; mobile computing uses communications technology to work in uncontrolled environments outside developer's premises
MSSR	Minimum Site Security Requirements, abbreviation for this document
Network architecture	Framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation
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

OS	Operating System
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
Policy	Set of security rules, procedures, or guidelines for an organization; a policy may pertain to a specific operational environment
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
SAM	Secure Access Module (or Secure Application Module)
SC & SD	Smartcard & Similar Devices where significant proportions of the required security functionality depend upon hardware (e.g. smart card hardware, smart card composite products, TPMs, digital tachographs, Host Security Modules, etc.)
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)

SW	Software
Team member	The term “team member” encompass employees, contractors, consultants, students, and third party users involved in the secure processes or having access to protected information
Teleworking	Working via remote access; teleworking uses communications technology to work remotely from a fixed location outside developer's premises
Third party user	Any user who is not employee, contractor, consultant, or student, e.g. customer, ITSEF, CB
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	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
VPN	Virtual Private Network; 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

40 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.

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

42 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.

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

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

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

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

4 Development Security System and Documentation

4.1 Objective

47 As required by ALC_DVS.1.1C and ALC_DVS.2.1C, respectively, the Development Security Documentation (DSD) shall describe the physical, logical, 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.

48 DSD shall identify all 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.

49 If ALC_DVS.2 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).

4.2 Policies

50 The evaluation evidence for the evaluation of development security is the ST and the development security documentation (DSD). Therefore, the developer has to 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.

51 The DSD shall document and the evaluator shall examine the development confidentiality and integrity policies that detail

- what information relating to the TOE development needs to be kept confidential, and which members of the development staff are allowed to access such material;
- what material must be protected from unauthorised modification in order to preserve the integrity of the TOE, and which members of the development staff are allowed to modify such material.

52 Policies shall contain a description of developers organization, relevant roles, and the security measures implemented. According to ALC_DVS the following types of security measures shall be considered for documentation

- Physical, e.g. access control and intrusion detection
- Procedural, e.g. granting and revoking access rights, transfer of protected material, roles and responsibilities for security personnel
- Personnel, e.g. check of trustworthiness
- Other security measures, e.g. logical protection of any development machines

4.3 Security Measures

53 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.

54 When justification is required (see 4.1) this document can be used as a basis after adaptation to the developer specific situation and environment.

55 The ability to demonstrate the link 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, can support both, ITSEF work packages and justification according to ALC_DVS.2.2C.

4.3.1 Control of documents

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

- approve documents for adequacy prior to issue;
- review and update documents as necessary and re-approve documents;
- ensure that changes and the current revision status of documents are identified;
- ensure that documents remain legible and readily identifiable;
- 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;
- prevent the unintended use of obsolete documents; and
- apply suitable identification to them if they are retained for any purpose.

4.3.2 Establishing and managing the DSS and DSD

57 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.

58 The developer is free to structure the DSD as appropriate. It may consist of the developers ISO27001 Information Security Management System, be structured according to this MSSR document, or be structured in any way suitable for the developer.

59 In order to support this ITSEF work package the developer 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.
- define the risk assessment approach of the organization including a risk assessment methodology that is suited to the DSS, the identified security, and legal and regulatory needs to protect the TOE,

  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.

- formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing security risks.
- implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.
- describe all selected control objectives and controls and their implementation, including the necessary processes and operation procedures.

60 The DSD should include:

- documented statements of the DSS policy and objectives;
- the scope of the DSS as far as the TOE is concerned;
- procedures and controls in support of the DSS;
- documented procedures needed by the organization to ensure the effective planning, operation and control of its developer security processes.

4.3.3 Monitor and review the DSS

61 The developer should

- execute monitoring and reviewing procedures and other controls to
  - promptly detect errors in the results of processing;
  - promptly identify attempted and successful security breaches and incidents;
  - enable management to determine whether the security activities delegated to people or implemented by technology are performing as expected;
  - help detect security events and thereby prevent security incidents by the use of indicators; and
  - determine if the actions taken to resolve a breach of security were effective.
- 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.
- review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks.
- conduct internal DSS audits at planned intervals defined in DSD.
- update security plans to take into account the findings of monitoring and reviewing activities.

4.3.4 Maintain and update the DSD

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

- should implement the identified improvements of the DSS in the DSD.
- should take appropriate corrective and preventive actions in accordance with 8.2 and 8.3.

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

4.3.5 Control of records

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

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

4.4 Examples

65 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.

66 Rules and regulations regarding document hierarchy, document structure, release procedures etc. are often defined in the Quality Management System according to ISO9000 series of standards. Usually, the QMS also defines the approach to preventive and corrective measures, audit schemes, and management review.

67 An Information Security Management System according to ISO27000 series of standards defines all necessary measure to preserve the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed. ISMS documentation refers to developer's ITIL and/or COBIT framework.

68 Where CC relevant activities are part of a bigger organization, special security measures are described in additional documentation. That may be additional chapters in the above mentioned documents, a dedicated document containing special regulations and referring to the above mentioned documents for all common regulations, or a dedicated DSD.

5 Management responsibility

5.1 Objective

69 The developer shall have well defined, documented, and assigned roles and responsibilities for all activities which may have an impact on confidentiality and integrity of the TOE.

70 All resources necessary to maintain confidentiality and integrity of the TOE shall be identified and available.

71 All physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE shall be effective.

5.2 Policies

72 The overall Security Policy shall define developer's approach to security and the area of applicability. It shall establish an overall sense of direction and principles for action with regard to confidentiality and integrity needs of the TOE.

5.3 Security Measures

73 Top Management (see 3) should define developer's legal and organizational structure and is responsible for confidentiality and integrity of the TOE.

5.3.1 Management commitment

74 Top Management 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.

5.3.2 Security Manager

75 The Security Manager(s) should 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' organization. The objectives and task of the Security Manager include but are not limited to the requirements described in chapter 4.

5.3.3 Resource management

76 The organization should determine (see 4.3.2) and provide the resources needed to satisfy the requirements set in this document. Determination should be updated regularly or after significant change of threats or environment.

77 Developer shall be responsible for all resources used regardless ownership.

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

79 All personnel, including members of external parties, shall be competent to perform the assigned tasks.

80 Where appropriate, organizational measures should ensure segregation of duties between development, production, testing, quality assurance, and security.

5.3.4 Confidentiality agreements

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

82 The necessary agreements should be concluded.

5.4 Examples

83 none

6 Internal DSS audits

6.1 Objective

84 Internal audits shall ensure that security measures are implemented in a meaningful and concerted way, and that security measures effectively support the intended purpose.

6.2 Policies

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

6.3 Security Measures

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

- conform to the requirements of this Requirement Document;
- conform to the identified security needs of the TOE;
- are effectively implemented and maintained; and
- are performing as expected.

87 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.

88 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.

6.4 Examples

89 none

7 Management review of the DSS (informative)

7.1 Objective

90 Management should ensure that developer has well defined, documented, and assigned roles and responsibilities for all activities which may have an impact on confidentiality and integrity of the TOE.

91 All physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE should be effective.

7.2 Policies

92 The management review process should be documented.

7.3 Security Measures

93 Management should review the organization's DSS at planned intervals, or when significant changes to the security implementation occur, in order 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.

7.3.1 Review input

94 The input to a management review should include

- results of DSS audits and reviews;
- feedback from interested parties, particularly Evaluation and Certification Bodies;
- status of preventive and corrective actions;
- vulnerabilities or threats not adequately addressed in the previous risk assessment;
- follow-up actions from previous management reviews;
- any changes that could affect the DSS; and
- recommendations for improvement.

7.3.2 Review output

95 The output from the management review should include any decisions and actions related to

- improvement of the effectiveness of the DSS.
- update of the risk assessment and risk treatment plan.
- modification of procedures and controls that effect security, as necessary, to respond to internal or external events that can impact the DSS.
- resources needed.

7.4 Examples

96 none

8 DSS improvement

8.1 Objective

97 Effectiveness of physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE shall be reviewed and improved where necessary.

8.2 Policies

98 Policies shall define how effectiveness of security measures is maintained despite evolving threats and in consideration of possible deficiencies.

8.3 Security Measures

8.3.1 Continual improvement

99 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.

8.3.2 Corrective action

100 The developer should take action to eliminate the cause of nonconformities with the DSS requirements in order to prevent recurrence.

8.3.3 Preventive action

101 The developer should determine actions to eliminate the cause of potential nonconformities with the DSS requirements in order to prevent their occurrence.

102 The developer should identify changed threats and define preventive actions focusing on significantly changed risks.

8.4 Examples

103 none

9 Control objectives and controls

9.1 Asset management

104 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).

9.1.1 Overall objective

105 Assets shall be clearly identified with the type of protection (confidentiality, integrity, authenticity) assigned, and managed.

106 Every asset shall have an owner.

9.1.2 Responsibility for assets

9.1.2.1 Objective

107 Ownership and acceptable use of assets shall be defined and deployed.

9.1.2.2 Policies

108 DSD should define ownership and management of all assets.

109 Rules for the acceptable use of information and assets should be identified and documented in line with the classification policies.

9.1.2.3 Security measures

110 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 in the development phase of its life cycle.

111 Developer should consider the list of important assets given in 9.1.2.4 when defining assets.

112 Inventories of the assets should be available and maintained.

113 Owners should be identified and nominated for all assets in the different stages of the development. Performing ownership must be evident for all owners. 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.

114 The rules for the acceptable use of information and assets should be strictly enforced, and verified in internal audits.

115 Assets, particularly computers, and all other equipment and materials provided by the developer should be used for official purposes only, and only according to the rules set in the DSS and related documents.

9.1.2.4 Examples

116 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/package, test program, initialization data, embedded software
- Card/Inlay manufacturing – modules, cards
- Personalization – cards/inlays, embedded software, data
- Shipment – reticle, wafer, modules/chips, cards/inlays
- Rejects and scrap may appear in all segments and should be considered assets.

117 Important assets beside the TOE or parts of it are typically:

- Security: access control and alarm system, keys, access codes
- Relevant information for the knowledge of the TOE: specifications, design documentation, guidance, source code, IC and embedded software representation, penetration tests results.
- Sensitive data used during the development phase of the TOE: keys, passwords, memory profile, integrity evidence.
- Information: databases, data files, contracts, system documentation, R&D information, archived information, production related data
- Software: R&D tools, applications, system software, development tools, CM systems
- Physical assets: computer equipment, communication equipment, removable media
- Services: computing and communications services, general utilities (power, air conditioning, lighting), storage and shipment

118 An asset inventory includes:

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

119 The asset 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.

120 Ownership is allocated for:

- all business processes
- Defined sets of activities
- Applications
- All defined sets of data
- Physical assets (premises, HW, networks etc.)

121 All information about assets are kept in appropriate databases.

9.1.3 Classification of information, data, and material

9.1.3.1 Objective

122 Assets shall receive an appropriate level of protection in line with its classification.

9.1.3.2 Policies

123 The developer shall have a classification policy.

124 The developer shall have predefined labelling and handling procedures for all used combinations of defined levels and information, data, and material implemented in accordance with the classification scheme adopted by the organization.

9.1.3.3 Security Measures

125 Assets should be classified according to an appropriate security level in terms of its criticality to the developer's organization and, particularly, to the intended area of application of any TOE concerned.

126 Classification relates to information, data, and material in any form.

- Hardcopy, e.g. documents, memos, presentations, drafts
- Electronic data, e.g. files, emails, software, development tools, CM systems, networks
- TOE and components (masks/reticules, wafer, dies, chips/modules, inlays, cards, demonstrators, samples, software etc.)

127 The classification scheme shall match with the classification as given in CEM AVA, paragraph 1975

- Public information concerning the TOE (e.g. as gained from the Internet);
- Restricted information concerning the TOE (e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement)
- Sensitive information about the TOE (e.g. knowledge that is shared between discreet teams within the developer organization, access to which is constrained only to members of the specified teams);
- Critical information about the TOE (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking).

- Very critical hardware design: The designs of modern ICs involves not only huge data bases but also sophisticated bespoke tools. Therefore, the access to useful data requires an enormous and time consuming effort which would make detection likely even with the support from an insider. If an attack is based on such knowledge the new level of "very critical design" has been introduced by JIL. It has to be decided in a case by case decision, if the knowledge cannot be gained in another way.

128 Classification should be in line with the factor "knowledge of the TOE" used to calculate an attack potential in the JIL application of Attack Potential to Smartcards.

129 A level of protection in accordance with the developer's classification policy should be associated with each asset.

130 The procedures for labelling and handling of information, data, and material should include, but are not limited to regulations regarding

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

131 The rules for labelling and handling should be strictly enforced.

132 Where confidentiality is required, 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 confidentiality of the TOE

133 Access to restricted information, i.e. classified "sensitive" or "critical", should only be granted on a need-to-know basis.

134 When a high level of security for especially critical material or operation is required, e.g. in case of classification "critical" or "or very critical", 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.

135 Information, data, and material considered sensitive, critical, or very critical shall be protected at any time.

136 The processes of destruction should be designed to provide full traceability of every piece of any tangible form of the TOE or its parts.

9.1.3.4 Examples

137 A typical classification scheme applies at least four levels of confidentiality, e.g.

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

138 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.

139 Destruction process:

- Wafer, single dies, and packaged chips are shredded in a rolling mill so that each edge of every 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 of manifestations of the TOE is recorded on CCTV.
- Confidential and strictly confidential documentation of the TOE on paper or optical disks are shredded according to at least DIN 66399, Security Class 3:
  - Paper class P6 (max. 0,78 mm x 11 mm strips)
  - Optical disks class O6 (max. 0,5 mm² residual area)
  - Magnetic disks class T6 (max. 10 mm²)
  - Hard disk drives class H6 (max. 10 mm²)
  - Electronic disks (sticks, SSD) class E6 (max. 1 mm²)
- Files on re-writable data carriers (HDD, SSD, USB sticks) are wiped according to US DoD 5220.22-M or destroyed as described above.

9.1.4 Rules for preserving integrity and authenticity of assets

9.1.4.1 Objective

140 Assets shall be protected against alteration or unauthorized modification.

9.1.4.2 Policies

141 The developer shall have predefined handling procedures for all important assets in line with protection needs.

142 Approach to and deployment of configuration management shall be defined in a policy.

143 Whenever parts of the TOE are imported from external sources, import procedures should define how developer enforces integrity and authenticity of the imported parts.

9.1.4.3 Security measures

144 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 Configuration Management 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. (Detailed requirements for CM systems are defined in CC part 3, ALC.)

145 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.

146 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.

147 Where technical measures are not applicable, organizational measures should be implemented, e.g. four-eyes-principle.

148 For data in transit, detection measures should be implemented, e.g. check sum, hash value, signature.

149 If imported parts stem from other secure development environments, integrity, authenticity, and – where required – confidentiality shall be protected during transfer. The import from untrusted sources should involve inspection of the imported parts if modification of these parts has the potential to compromise integrity of the TOE. This applies in particular to the transfer of ROM code, EEPROM content, or software related to the TOE.

9.1.4.4 Examples

150 none

9.2 Human resources security

9.2.1 Overall objective

152 The overall objective is to reduce the risk of theft, fraud or misuse of facilities by ensuring that employees, contractors, consultants, students, and third party users understand their responsibilities, and are suitable for the roles they are considered for.

9.2.2 Prior to employment

9.2.2.1 Objective

153 The developer shall grant access to assets only to trustworthy people.

154 The hiring and contracting process, respectively, shall ensure proper selection of team members.

9.2.2.2 Policies

155 DSD shall include policies for hiring and onboarding which ensure careful selection of trustworthy staff.

9.2.2.3 Security Measures

156 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.

157 As part of their contractual obligation, the team members shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for security.

158 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).

159 The same security requirements shall apply to employees moving from other areas within developers organization.

9.2.2.4 Examples

160 Respecting privacy regulations, developer make reasonable effort to gain confidence in the integrity of the staff 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.).

9.2.3 During employment

9.2.3.1 Objective

161 All team members shall be aware of information security threats and concerns and know their responsibilities and liabilities. They shall observe the rules and shall be equipped in order to support organizational security policies in the course of their normal work, and to reduce the risk of human error.

9.2.3.2 Policies

162 The developer shall have documents defining security roles and responsibilities of employees, contractors and third party users, in accordance with the organization's security policy (e.g. in job descriptions, project plans, contracts etc).

163 The approach to regular awareness training should be defined in a policy.

164 A policy should define monitoring measures implemented in order to detect irregular behaviour in line with local legislation.

9.2.3.3 Security Measures

165 Management shall require team members to apply security in accordance with established policies and procedures of the organization.

166 All employees of the organization and, where relevant, contractors and third party users should 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 should be kept, including date, attendances and content.

167 In order to identify security breaches monitoring records of security areas and secure networks, e.g. log files, should be analyzed in line with local legislation. 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.

168 An initial and regular (annual) security training program should 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. Process changes, learnings from security incidents and audits, and answers to frequently asked questions should be addressed in awareness trainings.

9.2.3.4 Examples

169 Developer’s management ensures that team members

- are properly briefed on their security roles and responsibilities prior to being granted access to sensitive areas, information, or information systems;
- are provided with guidelines to state security expectations of their role within the organization;

- achieve a level of awareness on security relevant to their roles and responsibilities within the organization;
- conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate working methods;
- continue to have the appropriate skills and qualifications;
- observe the rules; and
- lead by example.

170 The disciplinary process is used as a deterrent to prevent team members violating organizational security policies and procedures, and any other security breaches.

9.2.4 Termination or change of employment

9.2.4.1 Objective

171 Team members leave developer (termination of contract or change of employment) in an orderly and controlled manner in order to maintain integrity and/or confidentiality of assets and/or information.

9.2.4.2 Policies

172 The developer shall have appropriate procedures for employment termination and change of job, including revocation of access rights.

9.2.4.3 Security Measures

173 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.

174 All team members 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 a change of job assignment.

175 Access rights (physical and logical) of all team members 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.

176 The employment change/termination 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.

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

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

9.2.4.4 Examples

179 none

9.3 Physical and environmental security

9.3.1 Overall Objective

180 Physical security shall prevent unauthorized physical access to the organization's premises, secure areas, delivery and loading areas, assets, and information which may impair integrity or - where required - confidentiality of TOE.

181 Integrity and - for security systems - availability (see also 9.8) of security relevant equipment shall be ensured to prevent loss, damage, theft, compromise, or loss of integrity of assets and security controls.

9.3.2 Physical security perimeter

9.3.2.1 Objective

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

183 Protection 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.

9.3.2.2 Policies

184 A security policies shall define the two layer security concept and detail the concerted function of the two layers.

9.3.2.3 Security Measures

185 Stop Layer and Detection Layer shall be implemented in a concerted and meaningful way. Evidence should be provided that the resistance time value of the stop layer exceed the reaction time of supporting forces.

186 All openings towards the secured development area (e.g. air condition, cable ducts) shall be protected in order to effectively prevent intrusion.

187 Where buildings are not solely used for developers' activities, e.g. shared with other users from the same organization (support functions, manufacturing, R&D), the layers shall separate the different activities.

188 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.

189 In case that a physical manifestation of the TOE or its parts has a "self protection" mechanism this can contribute to or be considered as a stop layer. Details are laid out in the respective Exhibit.

9.3.2.4 Examples

190 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. digital CCTV). 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").

191 A Detection Layer consists 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

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

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

193 Development networks secured with strong access credentials and without TOE related data on local data carriers is considered a logical Stop Layer.

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

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

196 Air condition, cable ducts, etc. are protected with a welded metal grid.

9.3.3 Physical entry controls

9.3.3.1 Objective

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

9.3.3.2 Policies

198 An access control policy shall be in place, including regulations for visitors and contractors. Access shall only be granted on a need-to-know basis.

199 A policy shall define access regulations for service functions, e.g. housekeeping, facility management, cleaning staff.

200 Where applicable, policies shall detail access rights for officials and supporting forces, e.g. fire fighters.

9.3.3.3 Security Measures

201 Access requests shall be submitted in written or via an electronic work flow system.

202 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.

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

204 The access control system should be tamper proof.

205 Tailgating should be prevented by technical or organizational measures, depending on size and nature of the site, and the associated risks.

206 In high security areas strong authentication should be implemented.

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

208 Where full traceability is required (depending on the nature of activities) automated mantrap with strong authentication shall be implemented.

209 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.

9.3.3.4 Examples

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

211 The entire access control system with badge (e.g. smart card), reader, and backbone system is tamper proof. It runs on a separated, secured network. Mutual authentication of badge and reader prevents unauthorized read of access credentials. Communication between the different components of the access control system are secured by an appropriate protocol (e.g. OSDP V2). Encryption and key management are secured by a Secure Access Module (SAM).

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

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

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

9.3.4 Securing offices, rooms and facilities

9.3.4.1 Objective

215 Physical security for offices, rooms, and facilities shall be protected against unauthorised access.

216 Any intrusion shall be detected immediately.

9.3.4.2 Policies

217 A Policy shall detail measures implemented to ensure detection and prevention of unauthorised access to offices, rooms, and facilities. This shall include clear security procedures and safety regulations as well as - where applicable - outsourcing.

9.3.4.3 Security Measures

218 Intrusion detection and alarm systems shall be designed and applied. The development area should be alarmed and locked when unattended.

219 Access controlled doors and emergency exits should be monitored with magnetic contacts and CCTV, and the restricted rooms should be monitored with motion detection.

220 Easily accessible windows should be protected against intrusion.

221 Detection and monitoring systems should be connected to a security center with 24/7 operation. The security center shall have an appropriate level of security. The connection of all security devices (e.g. intrusion detection, CCTV) to the security center shall be protected against tampering. All security relevant processes shall be audited.

222 Where the security centre is housing the primary systems for CCTV monitoring, intrusion, fire, alarm control and access control:

- The following processes fall under relevant security processes
  - Access Control Management (rights to change badge access or create badges)
  - Activation and deactivation of security system
- The following processes are not considered as relevant security processes
  - View only access to CCTV
  - React only to security alarms with escalation to the company

9.3.4.4 Examples

223 Windows on ground floor or elsewhere reachable from a stand (roof, balcony, etc.) within 2.5 m are considered easily accessible.

9.3.5 Protecting against external and environmental threats

9.3.5.1 Objective

224 The security areas shall remain in a secure state and protect the TOE also in case of natural or man made disaster.

9.3.5.2 Policies

225 A disaster prevention and recovery policy is required, detailing the measures implemented to protect the TOE.

9.3.5.3 Security Measures

226 Appropriate physical protection against damage from fire, flood, and other forms of natural or man-made disaster should be designed and applied based on a risk assessment. Security systems like access control, CCTV etc. shall work even in case of natural or man-made disaster. This requirement also applies to logging and back-up systems.

9.3.5.4 Examples

227 none

9.3.6 Working in secure areas

9.3.6.1 Objective

228 Physical protection and guidelines for working in secure areas shall be designed and applied. Personnel shall be aware that information is only allowed to be shared on a need-to-know basis.

9.3.6.2 Policies

229 An access control policy based on need-to-know principle shall be developed, implemented, and maintained.

9.3.6.3 Security Measures

230 Access control rules and rights for each employee or visitor 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.

231 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 team members and are subject to the same security regulations as internals (see 9.2).

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

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

9.3.6.4 Examples

234 none

9.3.7 Public access, delivery and loading areas

9.3.7.1 Objective

235 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.

236 Visitors shall not get access to or insight into restricted areas or information unintentionally.

237 The TOE components shall be protected against tampering or theft during transit between physically separate secure areas.

9.3.7.2 Policies

238 The security policy shall consider that the design and layout of sites and premises should avoid high security areas next to public areas.

239 The security policy shall include a visitor regulation which has to be established, documented, and reviewed based on security requirements for access.

240 The security policy shall (if applicable) define measures to ensure that TOE components shall be protected against tampering or theft during transit between physically separate secure areas. Measures during transit shall correspond to the confidentiality and integrity classification.

9.3.7.3 Security Measures

9.3.7.3.1 Visitors

241 Visitors shall have only predefined, controlled access to the development environment. The routes and walkways designated to visitors should be designed to ensure that visitors will not see restricted areas or information unintentionally. 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.

9.3.7.3.2 Delivery and shipment

242 Areas for incoming deliveries and outgoing shipments should be separated; separation may be physically or temporarily.

243 Delivery and shipping areas shall be designed in a way 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).

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

245 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.

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

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

9.3.7.3.3 Transportation

248 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.

249 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.

250 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 if security measures are in place enabling recipient to undoubtedly identify origin of shipment.

251 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.

252 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
- Route and schedule
- Drivers name, truck license plate number

253 In order to prevent attacks shipment information should be encrypted.

254 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.

9.3.7.4 Examples

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

256 For ground transportation, the following rules are deployed:

- TOE or parts of it are packed in sealed transport boxes with unpredictable seal number (seal, plumb, or security tape)
- transport in a vehicle (commercial van, truck) with locked cargo area
- point-to-point transport without additional payload or hub/relation
- Two-man rule is applied during the entire transportation and the vehicle is not unattended at any time
- the transport is equipped with mobile phone and GPS based surveillance

9.3.8 Equipment security

9.3.8.1 Objective

257 Integrity and – for security systems - availability of security relevant equipment shall be ensured to prevent loss, damage, theft, compromise, or loss of integrity of assets and security controls.

9.3.8.2 Policies

258 A policy shall define handling and placing of security relevant equipment in order to protect against failures which could affect availability of those equipment, and interception or damage.

9.3.8.3 Security measures

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

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

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

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

263 Security measures should be applied to off-site equipment (Laptop, Mobile Phone, Handheld, Data carrier) taking into account 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.

264 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.

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

9.3.8.4 Examples

266 Equipment is located in areas minimizing unnecessary access into security areas. It is positioned to prevent unauthorized viewing.

267 Network cabling is protected from unauthorized interception or damage by avoiding routes through public areas. Cable run in cable ducts.

268 Access to switches and patch panels is restricted.

269 Classified information, data, and material is removed before maintenance. All maintenance is logged with date, time, and personnel involved.

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

9.4 Communications and operations management

9.4.1 Overall objective

271 Operations and communication related to TOE as well as to supporting infrastructures and resources shall be protected against internal and external threats.

9.4.2 Operational procedures and responsibilities

9.4.2.1 Objective

272 The TOE related operations shall be protected against unintentional or deliberate misuse of processing facilities or incorrect operations execution.

273 Infrastructure used to protect integrity and/or confidentiality of the TOE shall be secured.

9.4.2.2 Policies

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

275 Formal management responsibilities and procedures should be in place to ensure satisfactory control of equipment, software, or procedures, and all related changes.

276 A procedure shall define the level of separation between development, test and operational environments, and describe the controls implemented.

9.4.2.3 Security Measures

277 Developer should deploy an appropriate level of separation between development, test, and operational environment.

278 The correct usage of processing equipment and of operations execution should be facilitated by up-to-date operating procedure documentation.

279 Processing facilities should be subject to strict change management processes; changes should need authorization by management. When changes are made, an audit log containing all relevant information should be retained.

280 Utilizing or modifying assets without authorization or detection should be prevented by segregation of duties and areas of responsibilities. The following items should be considered:

- The initiation of an event should be separated from its authorization.
- The possibility of collusion should be considered in designing the controls.
- Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered.

9.4.2.4 Examples

281 Operating procedures and documented procedures for system activities are formal documents.

282 Documented procedures are available for system activities associated with information processing and communication facilities, such as computer start-up and shut-down procedures, back-up, equipment maintenance, media handling, computer room and mail handling management, and safety.

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

284 Change controls consider the following items:

- Identification and recording of significant changes;
- Planning and testing of changes;
- Assessment of the potential impacts, including security impacts, of such changes;
- Formal approval procedure for proposed changes;
- Communication of change details to all relevant persons;

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

285 Access to the access control system is segregated from handling of physical badges, e.g. assigned to HR and security guards, respectively.

9.4.3 Third party service delivery management

9.4.3.1 Objective

286 When third party services are used confidentiality and/or integrity of the TOE and its part shall be preserved.

9.4.3.2 Policies

287 Contract and vendor management policies shall define roles and responsibilities for managing the relationship with third parties.

9.4.3.3 Security measures

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

289 Service Contracts and Statements of Work should pass the developer's internal approval process. The Security Manager shall be involved and any feedback considered.

290 Third party services should be monitored and reviewed in order to check that security terms and conditions of the agreements are being adhered to, and that security incidents and problems are managed properly. A report should be kept as evidence.

9.4.3.4 Examples

291 none

9.4.4 System planning and acceptance

9.4.4.1 Objective

292 Systems planning shall minimize the risks of system failures for all systems supporting confidentiality and/or integrity of the TOE and its part.

9.4.4.2 Policies

293 A planning process for communication and operation systems shall be defined and documented.

294 Test procedures and acceptance criteria for new processing systems, upgrades, and new versions shall be established.

9.4.4.3 Security measures

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

296 New processing systems, upgrades, and new versions should be tested prior to acceptance ensuring that all acceptance criteria have been satisfied. Migration into production should require formal acceptance. The Security Manager shall be involved and heard.

297 Acceptance may include a formal certification and accreditation process to verify that the security requirements have been properly addressed.

9.4.4.4 Examples

298 none

9.4.5 Protection against malicious and mobile code

9.4.5.1 Objective

299 The integrity of systems and software supporting TOE related information shall be protected against malicious code where applicable.

9.4.5.2 Policies

300 A policy shall prohibit the use of unauthorized software.

301 A policy shall define compulsory protective measures to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium.

302 Management procedures and responsibilities shall be defined for malicious code protection on systems, including training in their use, alerting, reporting, and recovering from malicious code attacks.

303 A security policy shall define authorized mobile code operations.

9.4.5.3 Security measures

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

305 Computers and all other equipment and materials provided by the developer shall be used for company purposes only; exceptions may be defined for smart phone use. Downloading or storing unapproved software or data shall not be allowed.

306 Regular reviews of the software and data content of connected systems supporting critical business processes shall be conducted; the presence of any unapproved files or unauthorized amendments should be formally investigated.

307 Malicious code detection and repair software should be installed and regularly updated in order to scan computers and media as a precautionary control, or on a routine basis.

308 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.

309 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.

9.4.5.4 Examples

310 none

9.4.6 Back-up

9.4.6.1 Objective

311 Integrity, availability, and – where required – confidentiality of TOE related information and security systems (at least TOE related data, access control and administrator log files) shall be ensured when a back-up system is used.

9.4.6.2 Policies

312 A documented procedure approved by the Security Manager shall define secure back-up creation, storage, and destruction operations, ensuring the same level of security as for the original data.

9.4.6.3 Security measures

313 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.

314 Back-up arrangements should be regularly tested to ensure that they meet the requirements of the agreed back-up policy.

315 For critical systems, the back-up arrangements should cover all system information, applications, and data necessary to recover all TOE related and security systems in the event of a disaster.

9.4.6.4 Examples

316 The retention period for essential information and any requirement for archiving information permanently are determined.

317 Regular daily, weekly, and monthly back-up on data carrier (HDD, DVD, tape) is used by small entities. Large entities usually back-up data via online systems to remote locations or mirror data on redundant hot systems.

318 The security environment hosting back-ups provides the same level of security as the operational environment.

9.4.7 Network security management

9.4.7.1 Objective

319 Network security shall ensure adequate protection of TOE related data and information, and security infrastructure.

9.4.7.2 Policies

320 Developer shall specify network security in terms of network architecture and preventive and detective measures.

321 A policy shall restrict network traffic through the entry point into the development area’s network to its minimum.

9.4.7.3 Security measures

322 Network infrastructure security shall be based on implementation of the following security measures:

- Access restriction to authorized people only.

- Entry point control, restricting the traffic to a minimum.
- Separation from other network either physically or by VLAN technologies, protected by access control measures and appropriate firewall rules.
- Physical separation of hardware (e.g. server, firewall, router, patch panel, etc.) and administration into properly secured premises consistent with the security level of the development area.
- Strong authentication scheme defined for network access.
- Secured configuration of development machines with a controlled, restrictive user security policy that prevents the installation of additional, unauthorized functionality.
- Use of a mechanism between the corporate/public network boundary and the development area IT systems that provides up-to-date commercial grade protection against logical attacks.
- No wireless connectivity for development networks.

323 Network controls implementation should also consider the following items:

- Operational responsibility for networks separated from computer operations, e.g. network operation centre for administration of network devices and local administration of servers;
- 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
- Appropriate logging and monitoring to enable recording of security relevant actions;
- Management activities coordinate both, to optimize the service to the organization and to ensure that controls are consistently applied across the processing infrastructure.
- Members of the development environment should not have administrator rights on the IT systems which they work with.

324 It should not be possible to view and/or modify configuration items from outside the defined development area, even from within the corporate network.

325 Access to development networks should be limited to hardened client supplied by the developer. Development networks processing restricted information shall only permit remote access on hardened client specifically intended for this purpose via secure VPN. Development networks processing sensitive, critical, or very critical information shall not allow remote access from outside of the development network.

326 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.

327 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.

9.4.7.4 Examples

328 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

329 Common services (AD, DNS, license servers, etc.) are hosted in a DMZ. Network, server, and client administration is segregated.

330 Access to development networks is only possible with Thin Clients (terminals) or hardened clients which effectively prevent copying network content (e.g. no I/O except monitor, keyboard, and mouse).

9.4.8 Media handling

331 Storage media is used to both store data and to transport it from one location to another. Media may be tapes, HDD, USB Sticks, CD/DVD/BD, smartphones, smart cards, and any other data carrier.

9.4.8.1 Objective

332 In order to protect integrity and/or confidentiality of TOE related data and information, all media shall be protected against unauthorized disclosure, modification, removal, theft, destruction or damage.

9.4.8.2 Policies

333 Appropriate operating procedures should be established to protect documents, computer media, mobile devices, input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

334 Where confidentiality and/or integrity are required, procedures shall be in place for the management of removable media.

335 All procedures and authorization levels should be clearly documented.

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

9.4.8.3 Security measures

337 Media should be controlled and physically protected. Security measures should include appropriate media labelling, storage, safe transportation, disposal and handling that are necessary and vital to protect all forms of media used for the storage of data.

338 Classified data (restricted, sensitive, and critical) shall be encrypted while stored on movable data carrier and during transit.

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

340 Permission for removable media should be granted only if need is evident. Media should be stored in a safe, or a secure environment, in accordance with developer's specifications. Registration of removable media and a removal authorization process should be implemented in order to reduce opportunity for data loss and provide an audit trail.

341 Media containing non-public information should be stored and disposed of securely. Service providers for the collection and disposal services for papers, equipment and media should be selected carefully.

342 Disposal of sensitive items should be witnessed by developer's employees and logged as appropriate in order to maintain an audit trail.

343 When accumulating media for disposal, consideration should be given to the aggregation effect, which may turn a quantity of non-sensitive information into sensitive information.

9.4.8.4 Examples

344 An inventory provides the current status of all data media used for TOE related activities.

345 An approval process for removable media drives ensures that permission is granted only if need is justified. Records of removals are kept and an audit trail is maintained.

346 All media are stored in a safe when not in use.

347 Discarded optical disks (CD, DVD, BD) are shredded.

348 HDD are sanitized according to DoD 5220.22-M (3 passes) for further use within the organization.

349 The destruction process is logged and recorded on CCTV. Disposal of sensitive items is witnessed by developer's trustworthy employees.

9.4.9 Exchange of information

9.4.9.1 Objective

350 Integrity and - where required - confidentiality of information and data shall be maintained while exchanged within an organization or with any external entity.

9.4.9.2 Policies

351 Formal exchange policies, procedures, and measures shall be defined and deployed in order to protect the exchange of information through the use of all types of communication facilities.

9.4.9.3 Security measures

352 Data transfer to/from secured networks shall only be possible via secure mechanism with authorised access accounts. Appropriate measures shall be implemented to separate the external networks from the secured networks.

353 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.

354 Agreements should be established for the exchange of information and software between developer and external parties. Developer's policies, procedures, and standards should be referenced in such exchange agreements. The security content of any agreement should reflect the sensitivity of the business information involved.

355 Information involved in electronic messaging should be appropriately protected. Security considerations should include the following items:

- Protecting messages from unauthorized access (password, encryption) or modification;
- Ensuring correct addressing and transportation of the message;
- Ensuring authenticity of the message, i.e. sender/author of the message should be unambiguous;
- Strong authentication restricting access from publicly accessible networks, e.g. client certificate and VPN.

356 For shipment of data carrier and documents only company approved couriers should be used.

9.4.9.4 Examples

357 Exchange of documents or hardcopies is protected by utilization of locked containers or delivery by hand.

358 Tamper-evident packaging reveals any attempt to gain access.

359 In case of high security requirements, splitting of the consignment into more than one delivery and shipping on different routes can protect effectively.

9.4.10 Electronic commerce services

360 Not applicable

9.4.11 Monitoring

9.4.11.1 Objective

361 Unauthorized processing activities shall be detected.

9.4.11.2 Policies

362 A policy shall detail monitoring measures, particularly logging and assessment of log files.

9.4.11.3 Security measures

363 To allow detection of unauthorized processing activities, and to assist investigations, the following log files shall be produced and kept for a defined period of time:

- User activities, exceptions and information security events.
- System administrator and system operator activities.

- Denied login attempts or security breaches (by enabling the Security Event log function of all clients).
- Network related system activities from domain controllers, firewalls, or proxy servers.

364 Logging facilities and log information shall be protected against tampering and unauthorized access. The system administrator log files should be kept out of reach of the respective administrator or system operator, respectively, and checked at least monthly for suspicious activities.

9.4.11.4 Examples

365 Payment schemes require three months online, one year offline retention period for audit log files.

9.5 Access control to information systems

9.5.1 Overall Objective

366 Access (logical and physical) to information systems including access to business processes, to networks, to operating systems, to applications, and to information shall be controlled and restricted on a need-to-know basis.

367 Users, user roles, and user responsibilities shall be managed and controlled.

9.5.2 Business requirement for access control

9.5.2.1 Objective

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

9.5.2.2 Policies

369 An access control policy shall be established, documented, and regularly reviewed based on business requirements (security needs to protect confidentiality and/or integrity of TOE) for access. This policy shall detail access control rules for every role (user or group of users).

9.5.2.3 Security Measures

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

371 Access control roles for both, access to premises and access to systems, should be segregated, e.g. access request, access authorization, and access administration.

9.5.2.4 Examples

372 An access control policy takes into account

- security requirements of developers business activities;
- policies for information dissemination and authorization, e.g. the need-to-know principle and security levels and classification of information;
- consistency between the access control and information classification policies of different systems and networks;

- relevant legislation and any contractual obligations regarding protection of access to data or services;
- management of access rights in a distributed and networked environment which recognizes all types of connections available;

373 Roles in the access authorization process are segregated. Requests are approved by the applicant's manager and the system and/or data owner, authorization is implemented by a security manager (physical access) or an IT administrator (logical access), respectively. The access control system is managed by it's owner (security manager, application owner, system administrator).

9.5.3 User access management

9.5.3.1 Objective

374 Only authorized users shall be able to access information systems.

9.5.3.2 Policies

375 A policy regarding user access management shall be established and documented. It details how access rights and privileges are granted and the roles used.

376 A policy regarding password quality shall be established and documented.

9.5.3.3 Security Measures

377 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.

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

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

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

- 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.
- 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;
- 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;
- giving users a written statement of their access rights;

- requiring users to sign statements indicating that they understand the conditions of access;
- ensuring service providers do not provide access until authorization procedures have been completed;
- maintaining a formal record of all persons registered to use the service, e.g. Active Directory;
- immediately removing or blocking access rights of users who have changed roles or jobs, or left the organization;
- periodically checking for, and removing or blocking, redundant user IDs and accounts;
- ensuring that user IDs are not re-issued to other users.

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

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

383 The following steps shall be considered:

- 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;
- privileges shall be allocated to users on a need-to-use basis
- an authorization process and a record of all privileges allocated shall be maintained. Privileges shall not be granted until the authorization process is complete;
- the development and use of system routines should be promoted to avoid the need to grant privileges to users;
- the development and use of programs which avoid the need to run with privileges should be promoted.

384 The allocation of passwords shall be controlled through a formal management process. This process shall consider the following requirements:

- 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;
- establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;
- 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;
- temporary passwords shall be unique to an individual and shall not be guessable;
- passwords shall never be stored on computer systems in an unprotected form;

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

385 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.

386 Systems for managing passwords should be interactive and ensure quality passwords.

387 The password management system should

- store password files separately from application system data;
- store and transmit passwords in protected (e.g. encrypted or hashed) form.

388 Management shall review users' access rights at regular intervals using a formal process. The review of access rights shall consider the following guidelines:

- users' access rights should be reviewed at regular intervals, e.g. a period of 6 months
- users' access rights should be reviewed after any changes, such as promotion, demotion, or termination of employment;
- privilege allocations shall be checked at regular intervals to ensure that unauthorized privileges have not been obtained;
- changes to privileged accounts shall be logged for periodic review.

9.5.3.4 Examples

389 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.

390 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 are considered - where appropriate – to replace or complement passwords.

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

392 Users are required to sign a statement to keep personal passwords confidential; this signed statement is included in the terms and conditions of employment.

9.5.4 User responsibilities

9.5.4.1 Objective

393 User responsibilities for maintaining effective access control shall be clearly defined and users shall be aware of their responsibilities.

9.5.4.2 Policies

394 A policy shall detail users responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

395 A password policy shall require users to follow good security practices in the selection and use of passwords.

9.5.4.3 Security Measures

396 Developer shall follow good security practices in the selection and use of passwords.

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

- keep passwords confidential;
- avoid keeping a record
- change passwords at regular intervals or whenever there is any indication of possible system or password compromise;
- select quality passwords
- change temporary passwords at the first log-on;
- do not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- do not share individual user passwords;
- do not use the same password for business and non-business purposes.

398 Users shall ensure that unattended equipment has appropriate protection.

399 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.

400 Users should be advised to:

- terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
- log-off mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);
- 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;
- protect data stored on movable equipment by encryption of the persistent storage; where data is not encrypted movable equipment (notebook) should be secured by physical measures (e.g. with cable lock Kensington lock or kept in a locked cabinet) when not in use;
- keep data media locked unless encrypted.

401 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.

402 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).

9.5.4.4 Examples

403 The Password Policy requires users to:

- 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 (!"$%&/()=?*....);
- keep passwords confidential;
- store passwords securely utilizing an approved password safe;
- change passwords at regular intervals, e.g. every 90 days;
- change temporary passwords at the first log-on;
- do not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- do not share individual user passwords;
- do not use the same password for business and non-business purposes.

404 Unattended clients or workstations are protected by an activated, locked screensaver.

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

9.5.5 Network access control

9.5.5.1 Objective

406 Unauthorized access to networked services shall be prevented.

9.5.5.2 Policies

407 A policy regarding network access management shall be established and documented. It details the network architecture, network connections, network access control and other security measures.

408 Dedicated processes and guidelines for business partner access and interconnections with/to business partners shall be defined and documented.

9.5.5.3 Security Measures

409 Only devices controlled by developer shall be able to connect to the network.

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

- appropriate interfaces between the organization's network and networks owned by other organizations, and public networks;
- appropriate authentication mechanisms for users and equipment;
- control of user access to information services.

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

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

413 Where confidentiality of restricted information or only integrity is required remote access may be allowed with suitable security measures ensuring integrity and if applicable confidentiality on the same level of network security as in the developer's premises.

414 Automatic equipment identification should be used as a means to authenticate connections from specific locations and equipment. This control should be complemented with other techniques to authenticate the equipment's user. Equipment identification shall only be applied in addition to user authentication, not as replacement.

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

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

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

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

418 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.

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

420 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).

421 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. Routing controls shall be based on positive source and

destination address checking mechanisms. Security gateways should utilize at least either

- firewalls to validate source and destination addresses on the network layer;
- proxy server to validate source and destination addresses on application layer;
- SOCKS proxy server for user authentication.

422 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.

9.5.5.4 Examples

423 Network access is controlled by Network Access Control (NAC) systems, allowing access only for managed devices. NAC can be basic (using a local ID of the device, eg MAC address) or strong (using machine certificate and computer account in active directory).

424 Developer's network is separated from other networks by a DMZ with firewalls at either end.

425 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.

426 Equipment identification is used if it is important that the communication can only be initiated from a specific location or equipment. The identifier indicates whether or not this equipment is permitted to connect to a certain network. It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

427 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 while business partners and contractors without developer’s equipment get only restricted access to some applications hosted in the DMZ.

428 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.

9.5.6 Operating system access control

9.5.6.1 Objective

429 Unauthorized access to operating systems shall be prevented.

9.5.6.2 Policies

430 A policy shall be established and documented describing the measures taken to prevent unauthorized access to operating systems.

9.5.6.3 Security Measures

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

- authenticating authorized users, in accordance with a defined access control policy;
- recording successful and failed system authentication attempts;
- recording the use of special system privileges;
- issuing alarms when system security policies are breached.

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

433 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.

434 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.

435 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.

436 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.

9.5.6.4 Examples

437 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.

9.5.7 Application and information access control

9.5.7.1 Objective

438 Integrity and - where required - confidentiality of TOE related data and information, and security systems shall be protected through effective access control to applications and information.

9.5.7.2 Policies

439 A policy shall detail the measures taken to restrict access to applications and information, and to isolate systems with sensitive, critical, or very critical content.

9.5.7.3 Security Measures

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

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

442 Systems with sensitive, critical, or very critical content shall have a dedicated (isolated) computing environment.

443 Applications and systems with sensitive, critical, or very critical content (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.

9.5.7.4 Examples

444 none

9.5.8 Mobile computing and teleworking

9.5.8.1 Objective

445 TOE related data and information, and security systems shall be appropriately protected when using mobile computing and teleworking facilities.

9.5.8.2 Policies

446 A 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.).

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

9.5.8.3 Security Measures

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

449 Where confidentiality of restricted information or only integrity is required mobile computing may be allowed with suitable security measures ensuring integrity and if applicable confidentiality on the same level of network security as in the developer's premises.

450 Teleworking with access to the TOE or its parts, TOE related information, and related security systems shall only be allowed for environments with public or restricted content in absense of sensitive, critical, or very critical content. The teleworking environment (premises, IT etc.) shall meet all requirements related to integrity and - where applicable - confidentiality set in this document. If teleworking is permitted processes shall be in place to ensure integrity during all teleworking activities.

451 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 unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.

452 Teleworking uses communications technology to enable staff to work remotely from a location outside of the developers` environment. Mobile devices must be protected against logical attacks during access of external networks to the same extent as provided by the developers` network.

9.5.8.4 Examples

453 Remote access from the home office to developer's office environment is possible in order to check email and to use common office tools. Access to sensitive specifications, application notes etc. is not permitted.

9.6 Information systems acquisition, development and maintenance

9.6.1 Overall Objective

454 Security shall be an integral part of information systems. IT systems shall be secured to a level ensuring integrity and confidentiality of the TOE, and safeguarding availability and proper operation of security systems.

455 Information systems include operating systems, infrastructure, business applications (e.g. development environments, configuration management systems), and services, either off-the-shelf products or user-developed applications.

9.6.2 Security requirements for information systems (informative)

9.6.2.1 Objective

456 Security requirements should be identified and agreed upon prior to procurement of IT systems. Security should be an integral part of procurement requirements for information systems.

9.6.2.2 Policies

457 A procurement policy should define the steps necessary to mitigate risks from IT systems (HW and SW) in use.

458 Software development, implementation, and utilization of applications developed by or on behalf of developer should be detailed.

459 Installation and verification of off-the-shelf products should be defined.

9.6.2.3 Security Measures

460 All security requirements should 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.

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

462 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.

9.6.3 Correct processing in applications

9.6.3.1 Objective

463 Errors, loss, unauthorized modification, or misuse of information in IT systems shall be prevented.

464 Integrity and/or confidentiality of the TOE and its parts shall be ensured.

9.6.3.2 Policies

465 A policy shall detail measures implemented to ensure integrity and authenticity of data related to the TOE or to proper operation of security systems.

9.6.3.3 Security Measures

466 Appropriate controls should be designed into applications, including user developed applications, to ensure correct processing. These controls should be determined on the basis of security targets, other security requirements, and risk assessment. They should include the validation of input data, internal processing, and output data.

467 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.

9.6.3.3.1 Input data validation (informative)

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

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

9.6.3.3.2 Control of internal processing (informative)

470 The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity or confidentiality are mitigated. Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate.

9.6.3.3.3 Message integrity (informative)

471 The integrity of electronic mail communication should be ensured by using the encryption and signing functionality based on suitable cryptographic algorithms and appropriate protocols.

9.6.3.3.4 Output data validation (informative)

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

9.6.3.4 Examples

473 Checking input of data typically includes the following steps:

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

- periodic review of the content of key fields or data files to confirm their validity and integrity;
- inspecting hard-copy input documents for any unauthorized changes (all changes to input documents should be authorized);
- procedures for responding to validation errors;
- procedures for testing the plausibility of the input data;
- defining the responsibilities of all personnel involved in the data input process;
- creating a log of the activities involved in the data input process.

474 Control of internal processing may include:

- the use of add, modify, and delete functions to implement changes to data;
- the procedures to prevent programs running in the wrong order or running after failure of prior processing;
- the use of appropriate programs to recover from failures to ensure the correct processing of data;
- protection against attacks.

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

476 Output validation may include:

- plausibility checks to test whether the output data is reasonable;
- reconciliation control counts to ensure processing of all data;
- providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;
- procedures for responding to output validation tests;
- defining the responsibilities of all personnel involved in the data output process;
- creating a log of activities in the data output validation process.

9.6.4 Cryptographic controls

9.6.4.1 Objectives

477 Confidentiality, authenticity, and integrity of information shall be protected by cryptographic means. Cryptographic keys shall be managed and protected against disclosure, modification, loss, and destruction.

9.6.4.2 Policies

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

9.6.4.3 Security Measures

479 Cryptographic controls should be used to achieve different security objectives, including

- confidentiality: using encryption of information to protect sensitive, critical, or very critical information, either stored or transmitted;
- integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;
- non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

480 Encryption keys shall be based on open algorithms and be derived from a random with sufficient entropy to prevent brute force attacks.

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

482 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.

9.6.4.4 Examples

483 In 2012, German BSI requires at least 80 bits of entropy, i.e. 256 bit symmetric or 2048 bit asymmetric RSA key length.

484 A key management processes typically includes

- generating keys
- generating and obtaining public key certificates;
- distributing keys to intended users, including how keys are activated when received;
- storing keys, including how authorized users obtain access to keys;
- changing or updating keys including rules on when keys should be changed and how this will be done;
- dealing with compromised keys;
- revoking keys;
- recovering keys;
- archiving keys, e.g. for information archived or backed up;
- destroying keys;
- logging and auditing of key management related activities.

9.6.5 Security of system files

9.6.5.1 Objectives

485 Operating systems and applications shall be secured and protected against unintentional alteration. Access to program source code shall be restricted.

9.6.5.2 Policies

486 Administrator rights shall be regulated in a policy describing how they are granted, monitored, and revoked.

487 Access for vendors and service partners shall be detailed in a policy.

488 A policy shall define installation of software on operational systems, including developers approach to updates and patches.

489 A policy shall describe generation and utilization of test data, where applicable.

9.6.5.3 Security Measures

9.6.5.3.1 Control of operational software

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

- updating of the operational software, applications, and program libraries is performed by IT administrators upon IT internal processes.
- Users are not allowed to install software which is not approved by the developer.
- The process to add new software should include defined testing and release scenarios.
- 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.

491 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.

492 Physical or logical access for suppliers should only be granted for support purposes for the time necessary. The supplier's activities shall be monitored.

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

9.6.5.3.2 Protection of system test data

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

495 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.

9.6.5.3.3 Access control to program source code

496 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.

497 The TOE and its parts shall be controlled by a CM system (see 9.1.1.3).

9.6.5.4 Examples

498 none

9.6.6 Security in development and support processes

9.6.6.1 Objective

499 Security of applications, tools, and information shall be maintained.

500 Security applications and applications with impact on the TOE shall be controlled.

501 Applications developed by or on behalf of developer shall be fully compliant with specification and must not introduce any security weakness.

9.6.6.2 Policies

502 The release process for development applications and tools shall be documented.

503 A change management policy shall be defined and effective.

504 Perpetuation of confidentiality across applications, tools, and networks shall be documented.

9.6.6.3 Security Measures

9.6.6.3.1 Change control procedures

505 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.

506 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.

9.6.6.3.2 Technical review of applications after operating system changes

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

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

9.6.6.3.3 Restrictions on changes to software packages

509 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.

510 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.

9.6.6.3.4 Information leakage

511 Where confidentiality is required opportunities for information leakage shall be prevented.

9.6.6.3.5 Outsourced software development (informative)

512 Developer should monitor and control outsourced software development.

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

- licensing arrangements, code ownership, and intellectual property rights;
- escrow arrangements in the event of failure of the third party;
- contractual requirements for quality and security functionality of code;
- testing before installation to detect malicious code.

9.6.6.4 Examples

514 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.

515 Secure development lifecycle procedures are widely used to control software development.

9.6.7 Technical Vulnerability Management (informative)

9.6.7.1 Objective

516 Risks resulting from exploitation of published technical vulnerabilities should be mitigated.

9.6.7.2 Policies

517 A policy should detail developer’s approach to updating and patching.

9.6.7.3 Security Measures

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

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

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

9.6.7.4 Examples

521 none

9.7 Information security incident management

9.7.1 Overall Objective

522 Effective management of information security incidents shall ensure an appropriate level of security.

9.7.2 Reporting information security events and weaknesses

9.7.2.1 Objective:

523 All security related incidents and weaknesses shall be reported to the Security Manager in a manner allowing timely corrective action to be taken.

9.7.2.2 Policies:

524 The developer shall have a security incident management policy providing suitable feedback processes to ensure timely communication of security incidents. In particular, minimum criteria for reporting an event should be defined.

9.7.2.3 Security Measure

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

526 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.

527 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.

9.7.2.4 Examples

528 none

9.7.3 Management of information security incidents and improvements

9.7.3.1 Objective:

529 Information security incidents shall effectively be resolved and improvements shall be implemented in a timely manner.

9.7.3.2 Policies

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

9.7.3.3 Security Measures

531 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.

532 Every security incident should be documented in an access controlled, secured environment. Records should be maintained.

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

9.7.3.4 Examples

534 The respective policy describes the expected types of incidents, corresponding containment, and mitigation.

535 Types, volumes, and costs of information security incidents are quantified and monitored.

536 Where a follow-up action against a person or organization after an security incident involves legal action (either civil or criminal), evidence is 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 Overall objective

537 Business continuity management shall ensure uninterupted availability of processes, systems, and tools necessary to maintain the required level of security and/or integrity of the TOE and its part.

9.8.2 Security aspects of business continuity management

9.8.2.1 Objective

538 Integrity and - where required - confidentiality of the TOE and its parts shall be maintained in case of incidents, accidents, and crisis situations.

9.8.2.2 Policies

539 A managed process shall be developed and maintained for business continuity throughout the organization that addresses the security requirements.

540 Business continuity plans shall be documented and deployed in order 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..

9.8.2.3 Security Measures

541 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.

542 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.

543 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.

544 Where confidentiality is required, attention shall be put on the protection of the TOE in case of an incident. This should include, but is not limited to

- Automated shut down of IT systems;
- Automatically closing emergency exits;
- Deployment of additional security staff.

545 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.

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

9.8.2.4 Examples

547 none

9.9 Compliance (informative)

9.9.1 Overall Objective

548 Breaches of any statutory, regulatory or contractual obligations related to the TOE should be prevented.

9.9.1.1 Policies

549 A policy should detail developers approach to the identification of relevant legislation, statutory, regulatory and contractual requirements, third party intellectual property rights, and other applicable regulations.

9.9.1.2 Security Measures

550 It is necessary to identify relevant legislation, statutory, regulatory and contractual requirements, third party intellectual property rights, and other applicable regulations.

551 Developer should assign this task to appropriately trained employees or use external service providers.

9.9.1.3 Examples

552 none