

Statement of Applicability version 4 10/07/2015

Scope Statement: The delivery of data centre services

Clause	Security Control Category	Control	Description	Objective of Control	Implementation or Exclusion	Substantiation for inclusion/exclusion	Applicability
05 Information Security Policies	A.5.1 Management direction for information security	A.5.1.1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	Information Security Policy, following the guidance of ISO27002:2005, code of practice, on 7th June 2013 and has published this to all employees and shall do so to relevant external	Core requirement to comply with ISO27001, ISMS requirements	Applicable
05 Information Security Policies	A.5.1 Management direction for information security	A.5.1.2 Review of the policies for information	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	planned intervals, or earlier when significant changes may occur that could impact the suitability, adequacy and effectiveness of this policy for the stake holders	Core requirement to comply with ISO27001, ISMS requirements	Applicable
06 Organization of information security	6.1 Internal organization	A.6.1.1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	The Organization has clearly defined all information security responsibilities. Security roles and responsibilities of employees, contractors and third party users have been defined and documented as required by the Organization's information security policy.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business	Applicable
06 Organization of information security	6.1 Internal organization	A.6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	Duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of organizational assets	Part of existing business practice within the Organization, due to size of the organization this is limited	Applicable
06 Organization of information security	6.1 Internal organization	A.6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	Interxion entities maintain contact with relevant authorities	practice and guarantee continuous improvement of the organization's practice Control is selected in the Risk assessment Interxion HQ-ECSC, HQ-IT and Interxion Nederland BV	Applicable
06 Organization of information security	6.1 Internal organization	A.6.1.4 Contact with Special Interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	The organization maintains appropriate contact with special interest groups and other specialist security forums and professional associations	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-ECSC, HQ-IT and Interxion Nederland BV	Applicable
06 Organization of information security	6.1 Internal organization	A.6.1.5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	All Projects will be made aware of the need to address information security.	Interxion has both internal ICT and external CIM activity that is project related. These both have the ability to affect the operational security of Interxions Business	Applicable
06 Organization of information security	6.1 Internal organization	A.6.1.6 Management Commitment to Information Security	The Organization's management actively supports information security within the Organization through clear direction, demonstrated commitment, explicit assignment and acknowledgement of its – and everyone else's - information security responsibilities.	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	The Organization's management actively supports information security within the Organization through clear direction, demonstrated commitment, explicit assignment and acknowledgement of its – and everyone else's - information security responsibilities.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment HQ-ECSC, HQ-IT and Nederland BV	Additional
06 Organization of information security	6.2 Mobile devices and teleworking	A.6.2.1 Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	To ensure the security of teleworking and use of mobile devices.	A formal policy is in place and appropriate security measures have been adopted to protect against the risks of using mobile computing and communication facilities	Part of existing business practice within the Organization, through risk assessment the AUP has been extended Control is selected in the Risk assessment Interxion HQ-IT	Applicable
06 Organization of information security	6.2 Mobile devices and teleworking	A.6.2.2 Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	To ensure the security of teleworking and use of mobile devices.	A procedure and application form has been developed for home working activities and users are to comply with the AUP.	Part of existing business practice within the Organization, through risk assessment the AUP has been extended Control is selected in the Risk assessment Interxion HQ-IT	Applicable
07 Human resource security	7.1 Prior to employment	A.7.1.1 Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	employment, contractors and third party users are carried out in line with company guidelines and in accordance with the laws, regulations and ethics of [the Netherlands and local jurisdictions], and proportional to the Organization's business requirements, the classification of the information to be accessed, and the perceived	Through the company risk assessments, people are identified as high risk to the business and therefore the controls in part 8 have been adopted, if not already existing in current company practice. Control is selected in the Risk assessment Interxion HQ-ECSC and Interxion Nederland	Applicable
07 Human resource security	7.1 Prior to employment	A.7.1.2 Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	Employees, contractors and third party users must agree and sign the terms and conditions of their employment contract, which state their and the Organization's responsibility for information security	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
07 Human resource security	7.2 During employment	A.7.2.1 Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	Management requires employees, contractors and third party users to apply security in accordance with the policies and procedures of the Organization's ISMS	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business	Applicable
07 Human resource security	7.2 During employment	A.7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third-party users, shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	All employees of the Organization and, where relevant, contractors and third party users receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function	Through the company risk assessments, people are identified as high risk to the business and therefore the appropriate controls have been adopted, if not already existing in current company practice. Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
07 Human resource security	7.2 During employment	A.7.2.3 Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	The Organization has a formal disciplinary process for employees who have committed a security breach	Appropriate standard HR processes have been adopted, if not already existing in current company practice. Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
07 Human resource security	7.3 Termination and change of employment	A.7.3.1 Termination or change of employment responsibilities	There shall be a formal disciplinary process for employees who have committed a security breach.	To protect the organization's interests as part of the process of changing or terminating employment.	Responsibilities for performing employment termination have been clearly defined and assigned as defined in the company Joiners and Leavers Procedure	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland BV	Applicable
08 Asset Management	8.1 Responsibility for assets	A.8.1.1 Inventory of assets	shall be identified and an inventory of these assets shall be drawn up and maintained.	To identify organizational assets and define appropriate protection responsibilities.	It is Interxion policy to maintain accurate asset inventories. All relevant information assets are clearly identified, and an inventory of all important assets has been drawn up and is maintained.	Core requirement to comply with ISO27001, ISMS requirements. Core requirement of IFRS reporting requirements.	Applicable
08 Asset Management	8.1 Responsibility for assets	A.8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned.	To identify organizational assets and define appropriate protection responsibilities.	'owned' by a designated individual or part of the Organization ("Asset Owner") Details of the Asset are identified on the asset inventory. Within the Interxion organization each local entity is responsible for maintaining asset inventories	Core requirement to comply with ISO27001, ISMS requirements Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland BV	Applicable
08 Asset Management	8.1 Responsibility for assets	A.8.1.3 Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.	To identify organizational assets and define appropriate protection responsibilities.	Rules for the acceptable use of information and assets associated with information processing facilities have been identified, documented and implemented	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business. Control is selected in the Risk assessment Interxion HQ-IT Core requirement to comply with ISO27001, ISMS requirements	Applicable

Statement of Applicability version 4 10/07/2015

Scope Statement: The delivery of data centre services

08 Asset Management	8.1 Responsibility for assets	A.8.1.4 Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	To identify organizational assets and define appropriate protection responsibilities.	All employees, contractors and third party users are required to return all Organizational assets in their possession upon termination of their employment, as described in the Joiners and leavers procedure	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland BV	Applicable
08 Asset Management	8.2 Information classification	A.8.2.1 Classification guidelines	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	Information has been classified in terms of value, legal requirements, sensitivity and criticality to the Organization	Core requirement to comply with ISO27001, ISMS requirements	Applicable
08 Asset Management	8.2 Information classification	A.8.2.2 Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization..	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	An appropriate set of procedures for information labelling and handling has been developed in accordance with the classification scheme adopted by the Organization and this is set out in document the Document Management Manual.	Core requirement to comply with ISO27001, ISMS requirements	Applicable
08 Asset Management	8.2 Information classification	A.8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	Procedures for the handling and storage of information are set out in DOC 7.6 and DOC 10.15 to protect this information from unauthorized disclosure or misuse	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland BV	Applicable
08 Asset Management	8.3 Media handling	A.8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Interxion has set out guidelines on the use of removable computer media	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
08 Asset Management	8.3 Media handling	A.8.3.2 Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Media are disposed of securely and safely when no longer required	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
08 Asset Management	8.3 Media handling	A.8.3.3 Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	Guidelines are set out how the Organization ensures that media are protected against unauthorized access, misuse or corruption during transportation beyond the Organization's physical boundaries	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
09 Access control	9.1 Business requirements of access control	A.9.1.1 Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	To limit access to information and information processing facilities.	An access control policy has been established and is reviewed when required in the light of business and security needs	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
09 Access control	9.1 Business requirements of access control	A.9.1.2 Access to networks and network services	Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	To limit access to information and information processing facilities.	access to the services that they have been specifically authorized to use. The Organization protects its networked services in line with its access control policy, from unauthorized access.	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
09 Access control	9.2 User access management	A.9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights..	To ensure authorized user access and to prevent unauthorized access to systems and services.	granting and revoking access to all information systems and services. All users have a unique identifier (user ID) for their personal and sole use and a password authentication technique has been chosen to substantiate the claimed identity of a user	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
09 Access control	9.2 User access management	A.9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services..	To ensure authorized user access and to prevent unauthorized access to systems and services.	There is a formal user registration and de-registration procedure for granting and revoking access to all information systems and services	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
09 Access control	9.2 User access management	A.9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	To ensure authorized user access and to prevent unauthorized access to systems and services.	The allocation and use of privileges is restricted and controlled	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
09 Access control	9.2 User access management	A.9.2.4 Management of secret authentication information of users.	The allocation of secret authentication information shall be controlled through a formal management process	To ensure authorized user access and to prevent unauthorized access to systems and services.	The allocation of passwords is controlled through a formal management process	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
09 Access control	9.2 User access management	A.9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals	To ensure authorized user access and to prevent unauthorized access to systems and services.	Management reviews users' access rights at regular intervals using the formal process	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
09 Access control	9.2 User access management	A.9.2.6 Removal or adjustment of access rights	information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	To ensure authorized user access and to prevent unauthorized access to systems and services.	users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change in line with the Joiners and Leavers Procedure DOC 9.3	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ- IT	Applicable
09 Access control	9.3 User responsibilities	A.9.3.1 Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	To make users accountable for safeguarding their authentication information.	Users are required (By accepting the AUP) to follow good security practices in the selection and use of passwords	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
09 Access control	9.4 System and application access control	A.9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	To prevent unauthorized access to systems and applications.	Access to information and application system functions by users and support personnel is restricted	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
09 Access control	9.4 System and application access control	A.9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	To prevent unauthorized access to systems and applications.	Access to information systems is controlled by the secure log-on procedure	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
09 Access control	9.4 System and application access control	A.9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.	To prevent unauthorized access to systems and applications.	The password management system ensures quality passwords	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-IT	Applicable
09 Access control	9.4 System and application access control	A.9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled	To prevent unauthorized access to systems and applications.	Thid control is only applicable to the ICT team and it is the reponsibility of the Director of ICT to ensure that only authorised resources are able to utilise these programs. .	within the Organization. All ICT staff that have access to privileged utility programs are identified and controlled at the Active directory level. Users needing access to these programs can only be approved by the director of ICT.	Applicable
09 Access control	9.4 System and application access control	A.9.4.5 Access control to program source code	Access to program source code shall be restricted	To prevent unauthorized access to systems and applications.	Access to program source code is restricted	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-IT	Applicable

Statement of Applicability version 4 10/07/2015

Scope Statement: The delivery of data centre services

10 Cryptography	10.1 Cryptographic controls	A.10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	The use of Cryptographic controls is under development however best practice guidelines are followed.	Interxion applies cryptographic controls in the form of agreed standards for communication and transfer of information and data. All traffic within the company network is encrypted at a base level by the use of proprietary standards such as SSL where required. Remote access is further secured by two factor authentication. The use of data sticks and other removeable media is not covered by this policy.	Applicable
10 Cryptography	10.1 Cryptographic controls	A.10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	The use of Cryptographic controls is under development however best practice guidelines are followed.	application or usage scenario below requires a key (be it manual or automatically generated) :- Remote access – Users who wish to access Interxion systems remotely will follow the procedures laid out in ISMS 9.04 - Remote Access Procedure. Keys are automatically generated and destroyed on use.	Applicable
11 Physical and environmental security	11.1 Secure areas	A.11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	Interxion uses security perimeters to protect areas that contain information and information processing facilities.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.1 Secure areas	A.11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.1 Secure areas	A.11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	The Organization has designed and applied physical security for offices, rooms and facilities.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.1 Secure areas	A.11.1.4 Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	The Organization has designed and applied physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.1 Secure areas	A.11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	The Organization has designed and applied physical protection for working in secure areas	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.1 Secure areas	A.11.1.6 Delivery and loading areas	where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and isolated from information processing facilities to avoid unauthorized access.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.2 Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Part of existing business practice within the Organization	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Power and telecommunications cabling carrying data or supporting information services is protected from interception or damage	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.4 Equipment maintenance	Equipment shall be correctly maintained to enable its continued availability and integrity.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Equipment is correctly maintained to ensure its continued availability and integrity	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion Nederland BV	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Equipment, information or software may not be taken off-site without prior authorization	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ IT	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Security is applied to off-site equipment taking into account the different risks of working outside the Organization's premises	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ IT	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.7 Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ IT	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Users are required (as detailed in the Acceptable Use Policy) to ensure that unattended equipment has appropriate protection	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
11 Physical and environmental security	11.2 Equipment	A.11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	The Organization has adopted a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities and the requirement for compliance with this policy is set out in the AUP.	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
11 Physical and environmental security	11.3 Security reporting	A.11.3.1 Reporting security events	To ensure security events and weaknesses associated with physical and environmental security threats are communicated in a manner allowing timely corrective action to be taken.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Physical and environmental security events must be reported to the Manager Operations of the local entity as quickly as possible, as set out in DOC 11.1	extra control is appropriate and business continuity risk management requires that all events and weaknesses of physical and environmental security are reported Control is selected in the Risk assessment Interxion Nederland BV and Interxion HQ-ECSC.	Additional
11 Physical and environmental security	11.3 Security reporting	A.11.3.2 Reporting security weaknesses	To ensure security events and weaknesses associated with physical and environmental security threats are communicated in a manner allowing timely corrective action to be taken.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	All employees, contractors and third party users of information systems and services are required by DOC 11.1 to note and report to the Manager Operations of the local entity any actual or suspected weaknesses in Organizational systems or services	Interxion recognizes that due to the type of business it operates, this extra control is appropriate Control is selected in the Risk assessment Interxion Nederland BV and Interxion HQ-ECSC.	Additional
11 Physical and environmental security	11.4 Responding to Security Events	A.11.4.1 Responsibilities and procedures	To ensure a consistent and effective approach is applied to the management of physical security incidents.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	to ensure a quick, effective and orderly response to security incidents that ensures appropriate corrective or preventative actions, restores normal operations as quickly as possible, and ensures that improvement opportunities are identified and acted upon.	Interxion recognizes that due to the type of business it operates, this extra control is appropriate Control is selected in the Risk assessment Interxion Nederland BV and Interxion HQ-ECSC.	Additional

Statement of Applicability version 4 10/07/2015
Scope Statement: The delivery of data centre services

11 Physical and environmental security	11.4 Responding to Security Events	A.11.4.2 Learning from security incidents	To ensure a consistent and effective approach is applied to the management of physical security incidents.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	Incident reports shall be used for collecting data on security incidents and ECSCalation for the purpose of periodic review by the Information Security committee and the SVP Engineering & Operations Support of Interxion.	Interxion recognizes that due to the type of business it operates, this extra control is appropriate Control is selected in the Risk assessment Interxion Nederland BV and Interxion HQ-ECSC.	Additional
11 Physical and environmental security	11.4 Responding to Security Events	A.11.4.3 Collection of evidence	To ensure a consistent and effective approach is applied to the management of physical security incidents. Operating procedures shall be documented, maintained, and made available to all users who need them.	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	agreement with the managing Director of the local entity and the SVP Engineering & Operations Support of Interxion, judges if and when a follow-up action against a person or organization is required, irrespective of whether or not this would involve legal action (either civil or criminal) and evidence is collected, retained and presented to conform to the rules for evidence laid down with the laws of the respective area where the incident occurs.	Interxion recognizes that due to the type of business it operates, this extra control is appropriate Control is selected in the Risk assessment Interxion Nederland BV and Interxion HQ-IT and Interxion HQ-ECSC.	Additional
12 Operations security	12.1 Operational procedures and responsibilities	A.12.1.1 Documented operating procedures	processing facilities and systems that affect information security shall be controlled.	To ensure correct and secure operations of information processing facilities.	Operating procedures have been documented, are maintained and are made available to all users who need them	Part of existing business practice within the Organization	Applicable
12 Operations security	12.1 Operational procedures and responsibilities	A.12.1.2 Change management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	To ensure correct and secure operations of information processing facilities.	Changes to information processing facilities and systems are controlled	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business	Applicable
12 Operations security	12.1 Operational procedures and responsibilities	A.12.1.3 Capacity management	to reduce the risks of unauthorized access or changes to the operational environment.	To ensure correct and secure operations of information processing facilities.	ISMS DOC 12.10 sets out the Organization's approach to ensuring that the use of resources is monitored, tuned, and projections made of future capacity requirements to ensure the adequate system performance.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
12 Operations security	12.1 Operational procedures and responsibilities	A.12.1.4 Separation of development, testing and operational environments		To ensure correct and secure operations of information processing facilities.	Excluded	The Organization has very limited (to none) in-house software development and does not therefore require a separate development and test environment.	Not Applicable
12 Operations security	12.2 Protection from malware	A.12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	To ensure that information and information processing facilities are protected against malware.	malicious code and appropriate user awareness procedures have been implemented. The execution of mobile code must be authorized, the policy is that the configuration must restrict the mobility of the code to an intended environment avoiding such code violating the Organization's information security policies, and unauthorized mobile code is prevented from executing	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
12 Operations security	12.3 Backup	A.12.3.1 Information back-up	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy	To protect against loss of data.	The organization acts to identify and patch software and system	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
12 Operations security	12.4 Logging and monitoring	A.12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	To record events and generate evidence.	exceptions and information security events are produced. If any issues are highlighted, ICT management will decide if further and more in depth monitoring and retention of logs is required to assist in future investigations. All systems are monitored by the ICT department and any detected misuse is reported to the ICT manager. The results of the monitoring activities are reviewed on a regular base. Faults are logged via email to the ICT manager and it is the ICT manager's responsibility to ensure that the incident is analysed and appropriate action has been taken	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
12 Operations security	12.4 Logging and monitoring	A.12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	To record events and generate evidence.	Logging facilities and log information are protected against tampering and unauthorized access.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
12 Operations security	12.4 Logging and monitoring	A.12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed	To record events and generate evidence.	Logging facilities and log information are protected against tampering and unauthorized access. System administrator and system operator activities are logged at a same level as the default setting.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
12 Operations security	12.4 Logging and monitoring	A.12.4.4 Clock synchronisation	organization or security domain shall be synchronised to a single reference time source.	To record events and generate evidence.	The clocks of all relevant information processing systems within the organization are synchronized with an international time synchronization server.	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
12 Operations security	12.5 Control of operational software	A.12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	To ensure the integrity of operational systems.	The installation of software on operational systems is controlled	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-IT	Applicable
12 Operations security	12.6 Technical vulnerability management	A.12.6.1 Management of technical vulnerabilities	used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	To prevent exploitation of technical vulnerabilities.	Timely information about technical vulnerabilities of information systems used by the Organization is obtained, the Organization's exposure to those vulnerabilities evaluated, and procedure in place that sets out the measures taken to address the associated risks	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-IT	Applicable
12 Operations security	12.6 Technical vulnerability management	A.12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	To prevent exploitation of technical vulnerabilities.	Users are given the minimum access required. Clear rules are laid out in the AUP and associated ICT policies about how users can or cannot install software. users must read and accept the AUP.	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-IT	Applicable
12 Operations security	12.7 Information systems audit considerations	A.12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	To minimise the impact of audit activities on operational systems.	Audit requirements and activities involving checks on operational systems are carefully planned and agreed with appropriate management to minimize the risk of disruptions to business processes	Interxion adopts this control to ensure that any audit activity shall not impact our operations and therefore nor our services Control is selected in the Risk assessment Interxion HQ-IT	Applicable
13 Communications security	13.1 Network security management	A.13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.	To ensure the protection of information in networks and its supporting information processing facilities.	Networks are managed and controlled in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
13 Communications security	13.1 Network security management	A.13.1.2 Security of network services	all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	To ensure the protection of information in networks and its supporting information processing facilities.	Security features, service levels and management requirements of all network services have been identified and included in any network service level agreement, whether those services are provided in-house or outsourced and are managed	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable

Statement of Applicability version 4 10/07/2015

Scope Statement: The delivery of data centre services

13 Communications security	13.1 Network security management	A.13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	To ensure the protection of information in networks and its supporting information processing facilities.	Included	highest level the segregation can be described as there being three networks in the scope of this control. The first is the company network, within which Interxion employees utilise information and systems to carry out Interxion business. This network shall be designated "The ICT Office Infrastructure". the next is the "Data Centre Monitoring Infrastructure" and the final network is the wireless networks used by guests and customers. This shall be known as the "Unsecured Wireless Network" which shall be kept separate between the other networks.	Applicable
13 Communications security	13.2 Information transfer	A.13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	To maintain the security of information transferred within an organization and with any external entity.	Formal exchange policies, procedures and controls are in place to protect the exchange of information through the use of all types of communication facilities	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
13 Communications security	13.2 Information transfer	A.13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	To maintain the security of information transferred within an organization and with any external entity.	Agreements are established for the exchange of information and software between the Organization and external parties	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland BV	Applicable
13 Communications security	13.2 Information transfer	A.13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	To maintain the security of information transferred within an organization and with any external entity.	Information involved in electronic messaging is appropriately protected	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
13 Communications security	13.2 Information transfer	A.13.2.4 Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	To maintain the security of information transferred within an organization and with any external entity.	A confidentiality and non-disclosure agreement reflecting the Organization's requirements for the handling of information is in place and is reviewed regularly	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business. Control is selected in the Risk assessment Interxion HQ-ECSC, HQ-IT and Interxion Nederland BV	Applicable
14 System acquisition, development and maintenance	14.1 Security requirements of information systems	A.14.1.1 Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.	Statements of business requirements for new information systems, or enhancements to existing information systems, specify the requirements for security controls	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-IT	Applicable
14 System acquisition, development and maintenance	14.1 Security requirements of information systems	A.14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.	Excluded	Interxion does not use public networks for performing electronic commerce at present	
14 System acquisition, development and maintenance	14.1 Security requirements of information systems	A.14.1.3 Protecting application services transactions	protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.	Excluded	The protection of information of publicly available systems (limited to Interxion Corporate website) is part of existing business practice within the Organization. In the risk assessment process we have decided not	Not Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization	To ensure that information security is designed and implemented within the development lifecycle of information systems.	Excluded	This control is not relevant to Interxion business requirements as Interxion is not involved in on-line transactions at present	Not Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	To ensure that information security is designed and implemented within the development lifecycle of information systems.	The implementation of changes is controlled by the use of the formal change control procedures	The Organization has very limited (to none) in-house software development and does not therefore require a secure development policy at this time	Not Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	To ensure that information security is designed and implemented within the development lifecycle of information systems.	When operating systems are changed, business critical applications are reviewed and tested to ensure there is no adverse impact on organizational operations or security.	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	To ensure that information security is designed and implemented within the development lifecycle of information systems.	Excluded	Interxion has decided that this control is not relevant to Interxion business requirements as Interxion does not modify or develop application software packages	Not Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.5 Secure system engineering principles	documented, maintained and applied to any information system implementation efforts.	To ensure that information security is designed and implemented within the development lifecycle of information systems.	All Datacentre implementations will follow DT&EG Design Engineering Requirements	Interxion has decided that the scope of this control is limited to Data Centre design and implementation.	Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	To ensure that information security is designed and implemented within the development lifecycle of information systems.	Excluded	Interxion has decided that this control is not relevant to Interxion business requirements as Interxion does not modify or develop application software packages	Not Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development	To ensure that information security is designed and implemented within the development lifecycle of information systems.	Excluded	Interxion has decided that this control is not relevant to Interxion business requirements as Interxion does not outsource software development.	Not Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.8 System security testing	Testing of security functionality shall be carried out during development.	To ensure that information security is designed and implemented within the development lifecycle of information systems.	Excluded	Interxion has decided that this control is not currently relevant to Interxion business requirements as Interxion does not perform substantial development.	Not Applicable
14 System acquisition, development and maintenance	14.2 Security in development and support processes	A.14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	To ensure that information security is designed and implemented within the development lifecycle of information systems.	Acceptance criteria for new information systems, upgrades and new versions have been established and suitable tests of the system(s) are carried out during development and prior to acceptance	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business Control is selected in the Risk assessment Interxion HQ-IT.	Applicable
14 System acquisition, development and maintenance	14.3 Test data	A.14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled	To ensure the protection of data used for testing.	Test data is selected, protected and controlled	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-IT	Applicable
15 Supplier relationships	15.1 Information security in supplier relationships	A.15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	To ensure protection of the organization's assets that is accessible by suppliers.	All supplier relationships that involve access to Interxion resources or data will be assessed for risk. All supplier relationships will be periodically reviewed and where appropriate controls put into place within the agreements to mitigate risk	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business	Applicable
15 Supplier relationships	15.1 Information security in supplier relationships	A.15.1.2 Addressing security within supplier agreements	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	To ensure protection of the organization's assets that is accessible by suppliers.	communicating or managing organizational information assets or information processing facilities, or adding products or services to information processing facilities, contain or refer to all identified security requirements, and third parties are not allowed to access the Organization's information assets until such an agreement has controls to ensure that security requirements are established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. this control applies to tier 1 suppliers.	Part of existing business practice within the Organization and has been confirmed in latest risk assessment to remain relevant to the business	Applicable
15 Supplier relationships	15.1 Information security in supplier relationships	A.15.1.3 Information and communication technology supply chain	agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	To ensure protection of the organization's assets that is accessible by suppliers.		Control is selected in the Risk assessment Interxion HQ-IT and Interxion Nederland BV	Applicable

Statement of Applicability version 4 10/07/2015

Scope Statement: The delivery of data centre services

15 Supplier relationships	15.2 Supplier service delivery management	A.15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	To maintain an agreed level of information security and service delivery in line with supplier agreements.	Included as the review of supplier agreements is a part of Interxion business practice.	cooperation with the Senior Manager Quality and Compliance. All key supplier agreements are monitored regularly and periodic reports are generated both to assess service delivery performance but also to assure that security is maintained to levels agreed.	Applicable
15 Supplier relationships	15.2 Supplier service delivery management	A.15.2.2 Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks."	To maintain an agreed level of information security and service delivery in line with supplier agreements.	Included as the review of changes to supplier agreements is a part of Interxion business practice.	such a way to ensure adherence to the applicable portions of the information security policy. These processes are applied to ensure that the criticality of business and documented information is taken into account. additionally where applicable a risk assessment is carried out if changes to these agreements are felt to have an impact on the security of interxion and its services.	Applicable
16 Information security incident management	16.1 Management of information security incidents and improvements	A.16.1.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	to ensure a quick, effective and orderly response to information security incidents that ensures appropriate corrective or preventative actions, restores normal operations as quickly as possible, and ensures that improvement opportunities are identified and acted upon.	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
16 Information security incident management	16.1 Management of information security incidents and improvements	A.16.1.2 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	Information security events must be reported to the ICT manager along set procedure	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
16 Information security incident management	16.1 Management of information security incidents and improvements	A.16.1.3 Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	All employees, contractors and third party users of information systems and services are required to note and report to the ICT manager any actual or suspected weaknesses in Organizational systems or services	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
16 Information security incident management	16.1 Management of information security incidents and improvements	A.16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	security events. The process is designed to ensure the assessment of security events is unequivocal and clear. Management responsibilities and procedures have been established to ensure a quick, effective and orderly response to information security incidents that ensures appropriate corrective or preventative actions, restores normal operations as quickly as possible, and ensures that improvement opportunities are identified	Part of existing business practice within the Organization and identified in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
16 Information security incident management	16.1 Management of information security incidents and improvements	A.16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	to ensure a quick, effective and orderly response to information security incidents that ensures appropriate corrective or preventative actions, restores normal operations as quickly as possible, and ensures that improvement opportunities are identified and acted upon.	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
16 Information security incident management	16.1 Management of information security incidents and improvements	A.16.1.6 Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	The Director ICT is required to quantify and monitor the types, volumes and costs of information security incidents and shall report his findings on a regular base to the Information Security committee and the SVP Engineering & Operations Support of Interxion.	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
16 Information security incident management	16.1 Management of information security incidents and improvements	A.16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	with the SVP Engineering & Operations Support of Interxion, judges if and when a follow-up action against a person or organization is required, irrespective of whether or not this would involve legal action (either civil or criminal) and evidence is collected, retained and presented to conform to the rules for evidence laid down with the laws of the respective area where the incident occurs.	Part of existing business practice within the Organization and identified in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
17 Information security aspects of business continuity management	17.1 Information security continuity	A.17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Information security continuity should be embedded in the organization's business continuity management systems.	identified, along with the probability and impact of such interruptions, and the risk assessment process is extended to apply to business continuity risks. These risk assessments drive the business continuity planning framework	Core requirement to comply with ISO27001, ISMS requirements, company practice has now adopted this control as essential within the company business continuity planning	Applicable
17 Information security aspects of business continuity management	17.1 Information security continuity	A.17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Information security continuity should be embedded in the organization's business continuity management systems.	development and maintenance of business continuity throughout the Organization; it addresses the information security requirements needed for the Organization's business continuity. The Organization's BCP is developed. It enables the Organization 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, critical business processes.		
17 Information security aspects of business continuity management	17.1 Information security continuity	A.17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Information security continuity should be embedded in the organization's business continuity management systems.	A single framework of business continuity plans is maintained to ensure that the plan and all its sub-plans are consistent, to consistently address information security requirements, and to BCP's plans are developed for each entity of Interxion. Local entities are required to submit their respective BCP for approval to the SVP Engineering & Operations Support of Interxion Business continuity plans are tested and updated once yearly to ensure that they are up to date and effective	Core requirement to comply with ISO27001, ISMS requirements, company practice has been formalized further	Applicable
17 Information security aspects of business continuity management	17.2 Redundancies	A.17.2.1 Availability of information processing facilities	The organization shall implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Information security continuity should be embedded in the organization's business continuity management systems.	All systems in scope have been and will continue to be designed to ensure maximum availability. At a base level Interxion Design Engineering Requirements ensure that the physical systems that make up services are designed to standards deemed have an appropriate availability profile.	Core requirement to comply with ISO27001, ISMS requirements, company practice has been formalized further	Applicable
18 Compliance	18.1 Compliance with legal and contractual requirements	A.18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	All relevant statutory, regulatory and contractual requirements and the Organization's approach to meet these requirements have been defined, documented and are kept up to date for each information system and the Organization	verify, and where needed review and optimise the controls that assure the availability of information processing facilities. Currently the controls are applied to the following central finance systems. Note this control is a central ICT only control at this time.	Applicable
18 Compliance	18.1 Compliance with legal and contractual requirements	A.18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	Appropriate procedures have been implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable

Statement of Applicability version 4 10/07/2015
Scope Statement: The delivery of data centre services

18 Compliance	18.1 Compliance with legal and contractual requirements	A.18.1.3 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	The Organization's policy is to protect important records from loss, destruction and falsification, in accordance with statutory, regulatory, contractual requirements	in the latest risk assessment that the current process in place is relevant to the risk Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
18 Compliance	18.1 Compliance with legal and contractual requirements	A.18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	Data protection and privacy are ensured as required in relevant legislation, regulations and, where applicable, contractual clauses	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
18 Compliance	18.1 Compliance with legal and contractual requirements	A.18.1.5 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	compliance with relevant agreements . for avoidance of doubt these are limited to the AUP (ISMS 8.02 - Acceptable Use Policy) and the company Code of Conduct. This control is implemented in line with in country legislation and regulations.	with relevant agreements . for avoidance of doubt these are limited to the AUP (ISMS 8.02 - Acceptable Use Policy) and the company Code of Conduct. This control is implemented in line with in country legislation and regulations.	Applicable
18 Compliance	18.2 Information security reviews	A.18.2.1 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.	The Organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, rules, processes and procedures for information security) is independently reviewed at planned intervals, and if required when significant changes to the security implementation occur.	Core requirement to comply with ISO27001, ISMS requirements to ensure certification	Applicable
18 Compliance	18.2 Information security reviews	A.18.2.2 Compliance with security policies and standards	processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.	for their assets specifically ensure that all documented security procedures and work instructions within their area of responsibility are carried out correctly to achieve compliance with security policies and standards	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ-ECSC and HQ-IT and Interxion Nederland	Applicable
18 Compliance	18.2 Information security reviews	A.18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.	Information systems are regularly checked for compliance with security implementation standards and the Organization's technical compliance checking	Part of existing business practice within the Organization Control is selected in the Risk assessment Interxion HQ -IT	Applicable