

Number	Control
7.1	Prior to Employment
	Human Resource Management Security
	All candidates for employment, contractors and third party users should be adequately screened, especially for jobs with access to sensitive information. Background verification checks on all candidates (for jobs with access to sensitive information) for employment, contractors, and third party users should 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.
	Employees, contractors and third party who process information should sign an agreement (NDA) on their security roles and responsibilities.
8.3	Treatment of Media
	Information Life Cycle
	Information has to be destroyed in a timely and secure manner (<i>in accordance with the information classification policy</i>), taking into consideration the maximum and minimum legal retention terms of the destruction of data.
	Ensure that relevant audit logs and information associated with accounts are safeguarded in accordance to law and regulations or business requirements.
	Access Control
	Only accounts directly related to individuals are issued to employees. Requests for group accounts should be submitted to the Schiphol Cyber Security Center.
	A formal procedure exists for logical access security that limits the process of creating, changing and deleting and periodical checks of access rights to at least once a year. This procedure should contain at least the following elements: - written approval for requests, changes and deletion of data owners. The data owner has to indicate with which conditions an account gains access to a system and with which rights. - demonstrable timely removal (within 24 hours) as soon as access rights are no longer required or when end of employment or when role change. Disabling instead of removal ensure the audit logs remain relevant. - yearly check of distributed accounts, and quarterly check of inactive accounts - including administrative accounts (root, admin, etc.)
	Every quarter the information owner must check whether or not accounts have been active with a combination of undesirable transactions and whether accounts have been issued to persons who have left the organization. Results of these checks should be submitted for checks.
	30 days after the password has expired, the accounts will be automatically disabled.
	Functional management checks every quarter for accounts that have been inactive for 90 days or longer (dormant accounts). Dormant accounts have to be submitted to the manager of the employee. With the approval of the manager, the dormant account is to be de-activated immediately. If the manager does not reply within 14 calendar days, the accounts will be de-activated.

	Multi-factor authentication is to be used for all administrative access, including domain administrative access and all user accounts who have access to sensitive information on systems, this includes remote access through the internet.
	New services or applications, including external (cloud) solutions, must integrate with the IAM solution of Schiphol Group for account (user) and authorization (group/role) management. The use of open standard SCIM 2.0 is encouraged.
	Logging and Auditing
	A procedure is in place that ensures that the data owner identifies events that qualify for active logging, periodical monitoring and follow-up.
	It is mandatory to register the activities with at least the following attributes: account name, point of time, activity, system identification, network address where applicable. Activities refers to logons and log offs to the systems as well as failed logon attempts. Practicing the transactions is logged in the system.
	Logfiles are preventatively analyzed to ensure the identification of unwanted changes or transactions. Unwanted transactions are to be handled according to the incident response procedure.
	Auditlogs will be kept for at least 90 days, and are to be deleted after one year, or if applicable, after the term by law. Logging has to be connected to the SIEM solution of Schiphol. Controls have to be in place to ensure the integrity of the logs.
9.1.2	Access to Networks and Network Services
	All remote administration of servers, workstations, network equipment and similar systems has to happen through secured connections. Protocols such as telnet, VNC, RDP and others, that do not support strong encryption may only be used when they are protected by a secure encryption channel such as VPN.
	Computer systems are equipped with a (software) firewall that only allows the permitted network protocols. Prohibited services or traffic must be blocked and trigger an alarm.
	Privileged Account Management
	Management accounts: (1) are based on the least privilege principle, (2) are personal, (3) are only used when absolutely necessary, and (4) are registered.
	Allocating special access rights (root, admin, management) have to be checked quarterly to ensure that special access rights have not been obtained. The results of these checks should be administered, and the incident process needs to be started when unwanted issues are found.
	Administrators have to use their personal non-administrative accounts to login to a system, they can then, when needed, gain temporary access to their administrative privileges using, for example, sudo on Linux/UNIX, and Runas on Windows.
	Passwords
	New services or applications, including external (cloud) solutions, to be connected to the Single Sign-On (SSO) solution of Schiphol. Existing services or applications should preferably be connected to the SSO solution of Schiphol.

	The administration of passwords must comply with the following: (1) The identity of the person has been determined, (2) the password is secret for its entire lifecycle, (3) accounts de-activation after five unsuccessful attempts, (4) there is a limited re-use of passwords. (5) an initial password has to be changed, (6) new and temporary passwords are unique, (7) passwords always have to be transferred securely (encrypted), and (8) exceptions to password regulations have to be agreed upon by the Schiphol Cyber Security Center.
	Passwords for user accounts have to be strong, and must consist of at least eight characters, and include characters from at least three categories such as capital letter, numerals and special characters. These passwords have to be replaced after a maximum of 92 days.
	Passwords for administrative accounts have to be very strong, and must consist of at least 15 characters, and include characters from at least three categories such as capital letters, small letters, numerals and special characters. These passwords have to be replaced after a maximum of 180 days.
	Applications with which data can be processed are minimally secured with a name (accounts) and password combination.
	Passwords for service accounts have to be very strong, and must consist of at least 24 characters, and include characters from at least three categories such as capital letters, small letters, numerals and special characters. These passwords have to be replaced after a maximum of 3 years.
	Standard passwords and usernames such as those set by providers in systems and applications are to be changed at the first opportunity to a password that complies with administrative requirements for passwords. It is not allowed to use an IT system / application with the default passwords and user names by the provider. This applies to systems which are not used for production as well.
	Cryptography
	There has to be a Cryptographic Key Management (CKM) process / procedure, and this CKM needs to be explicitly approved by the Schiphol Cyber Security team.
	It is obligatory to use the centralized Schiphol Public Key Infrastructure (PKI) within the Schiphol Group domain or a certificate from a Certificate Authority (CA) approved by the Schiphol Cyber Security Center.
	All communication of sensitive information over public networks has to be encrypted.
	Sensitive information in rest (stored) has to be encrypted.
	Network traffic between the client and the internet server has to be rendered unintelligible to third parties via encryption (https, vpn, etc.)
	Passwords and user names must be stored as hash with a "salt" addition, and will only be sent through the network if strongly encrypted.
	An internet website uses a Security certificate issued by a public Certificate Authority (CA) such as Digicert, VeriSign, etc.. So called self-signed certificates are not permitted. It is preferred to use extended validation (EV) certificates, but this is not mandatory.
11.1	Secure Zones
	Physical Access Security

	<p>Computer systems and the cabling for data transport are only physically accessible for persons that have a legitimate reason. To ensure this there has to be a formal procedure for physical access security in which the process for the creation, change, removal and periodic check of access is registered. This procedure describes at least the following aspects and the demonstrability thereof:</p> <ul style="list-style-type: none"> - approval of request for changes by the data owner. - timely removal (within 24 hours) of access rights changes of these are no longer required, and at role change. - yearly check of given access rights. - accompaniment of third persons.
	Ambient conditions such as temperature and humidity are to be monitored and checked for circumstances that may negatively influence the functioning of information processing facilities.
	Equipment is to be protected against power cuts and other interruptions caused by disruptions in utilities.
	Equipment must have means of fire detection and repression, so that a fire can be signaled and extinguished in time to limit the damage to the ICT systems.
	A redundant data center server room has to be in another geographic risk area.
11.2	Equipment
11.2.2	Utilities
	Asset Management
	There has to be a procedure which describes how to deal with the loss and theft of a (mobile) device, including the remote deletion of the mobile device in case of loss or theft.
	Provide a mobile device with the option to erase the data remotely.
	Use approved hard disk encryption software for mobile devices and systems that (may) contain sensitive information. Approval happens on a per case basis by the Schiphol Cyber Security Center,
12.1	Management Activities and Responsibilities
12.1.1	Documented Management Activities
	Procedures are drafted for management activities that are related to information processing and communication facilities, the procedures for starting and shutting down or logging off systems, the maintenance of equipment, treatment of media, management and security of the computer areas, batch processing and mail processing.
12.1.2	Change Management

	<p>There is a must be a formal procedure for the management and changes which control the proces of request up to production, which applies to, amongst others, software, hardware and configuration changes, and to at least the following aspects and the demonstrability of:</p> <ul style="list-style-type: none"> - central registration of change requests and actual status - approval of requests - estimate of the impact of the changes (among other things on information security) - formal of a test plan per change (functional and technical) - registration of test results - formal approval for migration to production
12.1.3	Capacity management
	The capacity of production must be watched to discover incidents and errors. This should be done through the means of automated monitoring tools and following the console and logging.
12.1.4	Secure Software Development
	There must be a seperation between the development, test, acceptance and production environment, with procedures ensuring changes are implemented in a controlled manner in the production environment after these has been succesfully tested by someone not responsible for the development and the change.
12.2	Protection against malware
	Anti-malware
	All systems, servers and workstations have to have anti-malware management software installed. Signature have to be automatically updated, at least once every four hours.
	Use network based anti-malware for the identification of executables in all network traffic and ise technologies from signature based detection to detect anf filter malicious contents before it arrives at the target computer, etc.
	The anti-malware software needs to be configured so that all files that are received through public or external networks (such as partners) or storage media are checked for malware before usage.
	Business Continuity
	<p>There is a formal backup procedure describing processes that ensure:</p> <ul style="list-style-type: none"> - the backup scheme is defined for system and data owners and is designed and executed accordingly - backups on external locations (electronically) are stored - backups are protected against unauthorized physical and logical access.
	<p>Within the Schiphol Group the following standard for the formal backup procedure are as follows:</p> <ul style="list-style-type: none"> - Unstructured data: frequency: daily (once per 24 hours), retention term: 14 calander days - Systems that coincide financially with the month transitions: frequency: daily (once per 24 hours), retention time: 35 calander days. This also applies to cloud solutions. <p>These terms also apply as alternative when there is no RPO and RTO</p>

	There is a procedure that demonstrates at least once each year compliance with the agreed upon Recovery Point Objective (RPO) and Recovery Time Objective (RTO) after the loss (foreseen or unforeseen) of the availability of the information.
	Back-ups are protected with cryptography.
12.4.4	Time Synchronization
	System time is synchronized with the Schiphol Group time servers (NTP) unless the systems are not in th Schiphol offices or data centers, in which case other NTP servers can be used. Amongst other issues this ensures when recording an incident the chronology of the course of an incident is secured.
12.5	Management of Operational Software and Hardware
	Ensure that for all-in-house developed software the management is arranged and continuity of the service is guaranteed.
12.5.1	Installation of Software on Operational Systems
	Software is only allowed to be installed with the approval of the system owner; it is prohibited for end-users to install software without approval.
	Updating of production software, applications and databases, is only to be executed by trained administrators, and only after explicit approval of the Change Advisory Board (CAB).
	Applications and operatings systems are to be implemented only after extensive and successful tests. Tests are to cover the usability, security, effects on other systems and user friendliness.
	Software changes, including status, are to be centrally registered.
12.6.1	Management of Technical and Human Vulnerabilities
	<p>The management of the vulnerabilities of all systems, including those that are air-gapped, on firmware, BIOS, Operating System, middleware (such as database and webserver) and Hypervisor level are to be executed based on the vulnerability management procedure that amongst others:</p> <ul style="list-style-type: none"> - minimally monthly monitoring for new security patches as issues by the publisher, developer or programmer. - immediate installation of critical patches - installation of pachtes within 14 days after issueance of patches classified as high. -other patches are to be installed as the business processes allow
	All systems within the network are to be scanned on a monthly basis (or more friequently) with the aid of automated vulnerability scanning tools. For each systems a prioritized list of the most critical vulnerabilities is to be provided to the system owner. These findings are treated and solved within the set time.
	There is a demonstrable information security awareness program through which all employees are made conscious of at least the dangers of social engineering and data leakages, as well as how they can be prevented. There is an awareness program for security code development for developers.
13.1	Management of
13.1.1	Management Controls for Networks

	<p>It is not allowed to connect computer systems in two (or more) different logical or physical networks. A computer is allowed to have several network interfaces, but these are not allowed to be used in more than one logical networks. In this context a logical network is an ISO OSI layer 3/4 (TCP/IP) that is separated through subnets, routers, firewalls, etc.</p> <p>The only exception to this rule is a second connection on the (Schiphol Group) back-up network or management network.</p>
	<p>In case the network equipment and networks are in the Schiphol datacenters of Schiphol Group offices only the network equipment and networks provided by Schiphol Group (Schiphol Telematics) are to be used.</p>
	<p>Design and implement the network perimeter in a way that ensures all outgoing network traffic to the internet first passes through at least one application-layer proxy server. The proxy supports black and white listing of specific URLs, domain names and IP addresses.</p>
13.1.2	Protection of Network Services
	<p>All systems, including network components, are to be secured optimally on the basis of a security management system standard that gives substance to, amongst other issues, establishing the hardening policy and keeping it up-to-date. It also indicates which security configuration a system has to comply to (amongst others; BIOS, services, password requirements and domain policy).</p>
	<p>The hardening policy needs to be executed before a system or network component is put into production.</p>
	<p>The Schiphol Group follows the Center for Internet Security (CIS) benchmarks for hardening.</p>
	<p>As part of the network security management procedure for firewalls, it must be determined which firewall rules (filtering rules) are to be active. These need to be reviewed at least annually.</p>
13.1.3	Network Segregation
	<p>Networks are protected by segregated network domains. Segregation of networks is based on the value and classification of the information processed in the network (segment), level of trust, data owners and data processors.</p>
	<p>A public cloud or hybrid cloud (mix of private and public cloud) is only allowed after explicit consent of the Schiphol Cyber Security Center team, this solution is to be reviewed annually and requires the approval of this team.</p>
14.2	Security in Development and Supporting Services
14.2.1	Policy for Secure Development
	<p>Sensitive information, such as personal data, is not to be processed in a development, test and/or acceptance environment.</p>
14.2.8	Testing of System Security
	<p>Changes to production systems and applications are to be tested in a test environment before they are implemented in a production systems. Tests are never to be performed in a production environment.</p>
	<p>Schiphol retains the right to audit processes and controls in relation to a contract at least once per year. A third party statement by an independent auditor is among the options to realize this.</p>

	Agreements with suppliers are to include demands that relate to information security risks which relate to the supply chain of services and products in the field of information and communication technology.
15.1	Information security in supplier relationships
15.1.2	Incorporating security requirements into supplier agreement.
	All relevant information security requirements should be established and agreed with each supplier who has access for the information of the organization, whether they prepares, stores, communicates or offers.
16.1	Management of Information Security Incidents and Improvements
16.1.5	Response to Information Security Incidents
	<p>There is an incident response procedure that, amongst other aspects, includes:</p> <ul style="list-style-type: none"> - guidelines for the reporting and registering of incidents - guidelines for guarding the progress of follow-up on incidents - central registration of incidents including the status of this incident - periodic reports and analysis of the incidents to create controls which will prevent certain structural incidents.
18.1.4	Privacy and Data Protection
	Personal data is information that directly relates to a person or may be traced back to a person, as described in the Wbp and GDPR. In case a system processes personal data this needs to be reported to the Privacy Officer of Schiphol Group.
18.2	Information Security Reviews
18.2.2	Security Policy and Standards Compliance
	There has to be an inventory of which industry best practices or standards/sector agreements/laws or /(model) contracts/agreements are applicable on the data processed. These requirements must be met. As for example the PCI DSS.