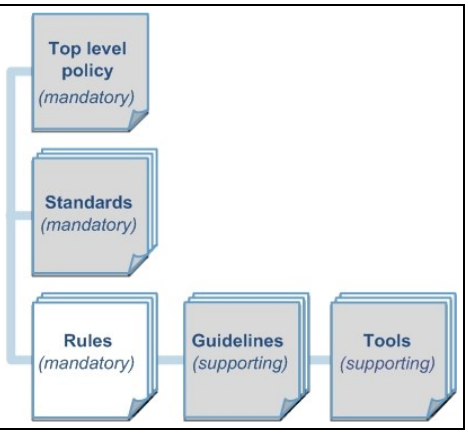
KPN Security Policy

KSP – Rule

Title	**(Web) Application Security**
ID	**KSP-FA05-RL11**
Funct. Area	05 - System & Network security
Date	29 July 2016
Version	v2.7
Status	Approved
Owner	CISO



Summary

This policy defines a set of policy rules regarding the protection of (web) applications.
These rules are based primarily on the OWASP Top 10 most critical web application security risks[1] and the Framework Secure Software by the Secure Software Foundation[2].

The rules provide security only under the assumption that an application runs on a system that is hardened according to KSP-FA05-RL04 System Hardening rule.

This policy is written for all KPN NL employees and managers who are involved in developing, maintaining and testing (web) applications. It concerns all applications owned by KPN or applications from vendors/partners that are used for KPN purposes.

[1] The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted.

[2] The Framework Secure Software is developed by the Secure Software Foundation. The framework is aimed at defining a method and controls that can be used to "measure" the security of software in an objective and repeatable manner.

Version history

Version	*Date*	*Comments*
v1.0	20 August 2013	Approved in SSM
v1.1	9 October 2013	Updated based on consistency check
v2.0	19 March 2014	Updated on several comments
v2.1	3 April 2014	Updated on comments from the CISO Red Team
v2.2	1 August 2014	Updated on several comments
v2.3	23 January 2015	Updated on several comments
v2.4	20 July 2015	Missing relevant requirements from the Framework Secure Software added and about defending against Clickjacking and Brute-Force attacks.
v2.5	13 November 2015	Version number incremented due to changes in the NL version
v2.6	29 April 2016	• Tightening of R20: 'all cookies' replaced by 'sensitive cookies' • Added R38 on setting the Strict-Transport-Security response header
v2.7	29 July 2016	• R07 broadened with direct expiration of existing session(s) after successfully changing credentials • R33 deleted because the requirement has no added value • R38 mentioning the possibility to include a domain in HSTS preload lists

ID	KSP-FA05-RL11-R01
Title	Preventing injection using a safe API
Description	A safe API must be used which avoids the use of the interpreter entirely or provides a parameterized interface.
Relating document	N/A

ID	KSP-FA05-RL11-R02
Title	Preventing injection using a non-parameterized API
Description	If a parameterized API is not available, special characters must be carefully escaped using the specific escape syntax for that interpreter.
Relating document	N/A

ID	KSP-FA05-RL11-R03
Title	Preventing injection using white list input validation routines
Description	Positive or “white list” input validation with appropriate canonicalization must be used (it is not a complete defense as many applications require special characters in their input).
Relating document	N/A

ID	KSP-FA05-RL11-R04
Title	Preventing Cross-Site Scripting and SQL Injections by escaping all untrusted data
Description	All untrusted data based on the HTML context (body, attribute, JavaScript, CSS, or URL) must be carefully escaped. This escaping must be included in applications unless the UI framework does this for them.
Relating document	N/A

ID	KSP-FA05-RL11-R05
Title	Preventing Cross-Site Scripting using white list input validation routines
Description	Positive or “whitelist” input validation must be used. Such validation should decode any encoded input, and then validate the length, characters, format, type and range on that data before accepting the input (it is not a complete defense as many applications require special characters in their input). Perform consistency checks at various stages of information being processed.
Relating document	N/A

ID	KSP-FA05-RL11-R06
Title	Strong authentication and session management controls
Description	A single set of strong authentication and session management controls must be used. For the requirements see Identity and access management standard and Password security rule.
Relating document	KSP-FA05-ST01 - Identity and access management KSP-FA05-RL01 - Password security

ID	KSP-FA05-RL11-R07
Title	Use strong session tokens and protect these
Description	• Session tokens may not be predictable and able to (reasonably) withstand brute-forcing attacks. • Session tokens must be linked to a unique user as much as possible (e.g. linked to IP address, SSL tokens, MAC address, etc.) to prevent hijacking. • Session tokens must not be exposed through other channels. • Session IDs must be strong, temporary, replaced after logging in and deleted with a timeout on the server side. • All existing session tokens/active sessions must directly expire once credentials have been successfully changed, so that existing sessions on other devices/apps/etc. (based on the old account information) will not remain valid until the normal session expiration time.
Relating document	N/A

ID	KSP-FA05-RL11-R08
Title	Indirect Object References per user or session
Description	Object references should not be predictable and able to withstand brute-forcing attacks. • Per user or session indirect object references must be used. • The application must map the per-user indirect reference back to the actual database key on the server.
Relating document	N/A

ID	KSP-FA05-RL11-R09
Title	Check Access when using Direct Object References
Description	Each use of a direct object reference from an untrusted source must include an access control check to ensure the user is authorized for the requested object.
Relating document	N/A

ID	KSP-FA05-RL11-R10
Title	Preventing Cross-Site Request Forgery (CSRF)
Description	CSRF tokens may not be predictable and must be able to (reasonably) withstand brute-forcing attacks. An unpredictable token must be included in the server response, preferably in a hidden field in the form body. This token must be returned by the client and validated by the server. Such tokens must at a minimum be unique per user session, but can also be unique per request.
Relating document	N/A

ID	KSP-FA05-RL11-R11
Title	Updating and patching of the (web) application
Description	All source code, including libraries that are used for generating the (web) application must be regularly updated and patched. Application (code) moving into production must be security tested via code reviews (adhere to OWASP Secure Coding practices) or penetration tests.
Relating document	KSP-FA05-ST02-R08 (Vulnerability Management)

ID	KSP-FA05-RL11-R12
Title	Application security architecture
Description	The application security architecture must provide good separation and security between components: at any level of an application stack, including the platform, web server, application server, framework, and custom code.
Relating document	N/A

ID	KSP-FA05-RL11-R13
Title	Encryption of sensitive data at rest
Description	Encrypt all sensitive data at rest in a manner that defends against threats. For the requirements see Cryptography rule. For information classification see Classification of information rule.
Relating document	KSP-FA05-RL07 - Cryptography KSP-FA03-RL01 - Classification of information

ID	KSP-FA05-RL11-R14
Title	Encryption of offsite backups
Description	Ensure offsite backups are encrypted, but the keys are managed and backed up separately. For the requirements see Cryptography rule. For guidelines on backup and restore see Backup guideline.
Relating document	KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL11-R15
Title	Strong standard algorithms and keys
Description	Ensure appropriate strong standard algorithms and strong keys are used to protect sensitive data, and key management is in place. For the requirements see Cryptography rule.
Relating document	KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL11-R16
Title	Passwords
Description	Ensure passwords are hashed with a strong standard algorithm and an appropriate salt is used. For the requirements see Cryptography rule.
Relating document	KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL11-R17
Title	Proper authentication and authorization for each page
Description	The enforcement mechanism(s) must deny all access by default, requiring explicit grants to specific users and roles for access to every page.
Relating document	N/A

ID	KSP-FA05-RL11-R18
Title	Page authorization in a workflow
Description	If the page is involved in a workflow, it must be verified that conditions are in the proper state to allow access.
Relating document	N/A

ID	KSP-FA05-RL11-R19
Title	Transport Layer Protection using SSL
Description	All pages with sensitive data must use SSL. Also, the location to which sensitive data is being posted to must use SSL without redirection from a non-SSL target. Pages containing sensitive data are: - pages displaying sensitive information, e.g. information impacting the privacy of the end-user. - pages which are used for consuming sensitive information, e.g. login forms. Possible exception: when a redirect from the non-SSL location to the SSL location ensures that the end-user is not capable of using the unsecured page.
Relating document	KSP-FA05-RL07 - Cryptography KSP-FA05-TL02 - Cryptographic algorithms and cipher suites

ID	KSP-FA05-RL11-R20
Title	Transport Layer Protection: sensitive cookies
Description	The HttpOnly and Secure flag must be set on sensitive cookies.
Relating document	N/A

ID	KSP-FA05-RL11-R21
Title	Transport Layer Protection using strong algorithms only
Description	Use transport layer security services that are provided by validated cryptomodules. See Cryptography rule and the Cryptographic algorithms and cipher suites tool.
Relating document	KSP-FA05-RL07 - Cryptography KSP-FA05-TL02 - Cryptographic algorithms and cipher suites

ID	KSP-FA05-RL11-R22
Title	Transport Layer Protection: certificate validation
Description	Certificates must be centrally managed, valid, not expired and not revoked. Certificates must also be valid for the domains they serve.
Relating document	http://tools.ietf.org/html/rfc5280 http://tools.ietf.org/html/rfc2818 KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL11-R23
Title	Transport Layer Protection: backend and other connections
Description	Backend and other connections must also use SSL or other encryption technologies.
Relating document	KSP-FA05-RL07 - Cryptography

ID	KSP-FA05-RL11-R24
Title	Involvement of user parameters in calculating the destination in redirects and forwards
Description	Don’t involve user parameters in calculating the destination in redirects and forwards.
Relating document	N/A

ID	KSP-FA05-RL11-R25
Title	Mapping values as destination parameter
Description	If destination parameters can't be avoided, the supplied value must be valid, and authorized for the user. Any such destination parameters must be a mapping value, rather than the actual URL or portion of the URL, and the server side code must translate this mapping to the target URL.
Relating document	N/A

ID	KSP-FA05-RL11-R26
Title	Reference to responsible disclosure page
Description	A reference to the responsible disclosure page on KPN.com must be included. This reference should be no more than one click away from the main page.
Relating document	N/A

ID	KSP-FA05-RL11-R27
Title	Maintaining the integrity of information processed
Description	The integrity of information processed by applications must be maintained by ensuring that: • information is not corrupted when modified by more than one user • information cannot be overwritten accidentally • the processing of information is validated • changes to key 'static' information such as customer master files or currency exchange rates are reviewed • unauthorised or incorrect changes to information are detected
Relating document	N/A

ID	KSP-FA05-RL11-R28
Title	Preventing inaccurate entry of information
Description	Inaccurate entry of information must be prevented by: • Only accepting data from trusted and authenticated information sources for data changes (creation, change, deletion) • New records have initialization values • Using error messages
Relating document	N/A

ID	KSP-FA05-RL11-R29
Title	Output validation
Description	Output validation routines must be used to allow a reader or subsequent processing system to determine if output is within predefined data range and all data is processed.
Relating document	N/A

ID	KSP-FA05-RL11-R30
Title	Revealing application or system information
Description	The application must not reveal server side information such as IP address, server name and other system information that could aid an attacker. Unnecessary application or system information such as stack traces, codes and parameters must not be disclosed when the application encounters an error.
Relating document	N/A

ID	KSP-FA05-RL11-R31
Title	Session Timeout
Description	When a user does not perform any action on a web site during a certain interval (defined by the web server) the status of the user session on the server side must be changed to "not used anymore" and instruct the web server to destroy the user session (deleting all data contained into it). • Set session timeout to the minimal value possible depending on the context of the application. • Avoid "infinite" session timeout. • The session cookie must expire when the browser is closed.
Relating document	N/A

ID	KSP-FA05-RL11-R32
Title	Security requirements and functional threats
Description	All security requirements must be thoroughly defined as well as at least one functional threat per requirement.
Relating document	N/A

ID	KSP-FA05-RL11-R34
Title	Secure coding standard
Description	A secure coding standard must be used and the software system's code must follow this standard.
Relating document	N/A

ID	KSP-FA05-RL11-R35
Title	Areas of expertise
Description	The development team must have the necessary areas of expertise, or be able to hire specialists when this expertise is not available, to perform the developer actions prescribed by this policy.
Relating document	N/A

ID	KSP-FA05-RL11-R36
Title	Defending against Clickjacking
Description	Clickjacking must be prevented by: • Sending the proper X-Frame-Options HTTP response headers that instruct the browser to not allow framing from other domains or/and • Employing defensive code in the User Interface to ensure that the current frame is the most top level window
Relating document	N/A

ID	KSP-FA05-RL11-R37
Title	Brute-Force protection
Description	Internet facing applications must protect its (user) accounts from brute-force attacks. A process must be in place to detect abusive behavior and a process must be in place to react upon the abuse. Possible actions: • Detect (rapid) automated login attempts and react by blocking the IP address temporarily. Report to SOC. • After detecting abusive behavior; force the account to logon with a CAPTCHA. Report to SOC. • After detecting abusive behavior; force the account to logon with a second factor. This option assumes there is an opportunity to use SMS or another out of band communication method. Report to SOC.
Relating document	N/A

ID	KSP-FA05-RL11-R38
Title	Support HTTP Strict Transport Security (HSTS)
Description	Set the Strict Transport Security response header. The Strict-Transport-Security response header tells the browser to not accept any untrusted, expired, or revoked TLS certificate from the domain. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS. It also prevents HTTPS click through prompts on browsers. Most major browsers (IE 11 and Edge, Firefox, Chrome, Opera, Safari) also have HSTS preload lists. Be aware that inclusion in the preload list cannot easily be undone. Don't request inclusion unless you're sure that you can support HTTPS for your entire site and all its subdomains the long term.
Relating document	N/A