REF		Maatregel	Fase	Type	Prioriteit	Uitwerking	Verwachtwoordelijke	Inspanning
		1. Beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van maatregelen en procedures						
7.1.1	1	Het management van de organisatie stelt het informatiebeveiligingsbeleid, inclusief dat ter zake van de beveiliging van persoonsgegevens, vast en draagt dit beleid uit binnen de organisatie.	Beheer	Procedureel				
7.1.2	1	In het informatiebeveiligingsbeleid worden de volgende onderwerpen opgenomen:	Beheer	Procedureel				
7.1.2a	1	Een definitie van de term informatiebeveiliging, de doelstellingen en het belang van de informatiebeveiliging als een instrument voor het realiseren van de zorgvuldige en effectieve maatregelen met betrekking tot een betrouwbare, continue en exclusieve verwerking van persoonsgegevens;	Beheer	Procedureel				
7.1.2b	1	De organisatie van de informatiebeveiligingsfunctie, waaronder de verantwoordelijkheden, taken en bevoegdheden voor alle aspecten van informatiebeveiliging en de verantwoordelijkheid ervoor bij het management;	Beheer	Procedureel				
7.1.2c	1	Een verplichting voor het management om de implementatie van de procedures en maatregelen in de organisatie te realiseren en te beheren;	Beheer	Procedureel				
7.1.2d	1	De wijze waarop het beveiligingsbewustzijn vanuit het management wordt overgedragen aan de organisatie en de instandhouding ervan;	Beheer	Procedureel				
7.1.2e	1	De onafhankelijke beoordeling van de toereikendheid van het beleid, alsmede de tactische en operationele uitvoering daarvan;	Beheer	Procedureel				
7.1.3 a	1	Medewerkers worden expliciet geïnformeerd over de aanwezigheid en het gebruik van persoonsgegevens die worden gegenereerd in het kader van de uitvoering van en de controle op de naleving van de maatregelen voor informatiebeveiliging (bewustzijn).	Beheer	Procedureel				
7.1.3 b	1	Vertrouwelijke informatie betreffende de naleving en handhaving van de beveiligingsmaatregelen mag niet in handen komen van een niet-geautoriseerde ontvanger.	Beheer	Procedureel				
7.1.4	1	Regelmatig rapporteert de daarvoor aangewezen persoon aan de hoogste autoriteit (de verantwoordelijke in termen van de WBP) in de organisatie over de naleving van het beleid van de beveiliging van persoonsgegevens en de invulling daarvan binnen de organisatie.	Beheer	Procedureel				
7.1.5	1	De verantwoordelijke zorgt ervoor dat invulling wordt gegeven aan het beleid voor de beveiliging van persoonsgegevens. Daarna dient een implementatieplan te worden opgesteld. Hierbij kan onderscheid worden gemaakt tussen een plan voor informatiebeveiliging en, indien de gewijzigde omstandigheden daartoe aanleiding geven, een plan voor een bepaalde planperiode. Kleinere organisaties kunnen wellicht volstaan met een vereenvoudigde vorm van een dergelijk plan.	Beheer	Procedureel				
7.1.6	1	Bij het opstellen van een beveiligingsplan wordt aandacht besteed aan:	Beheer	Procedureel				
		1. het verankeren van de activiteiten voor beveiliging van persoonsgegevens in de dagelijkse werkzaamheden van de medewerkers van de organisatie;	Beheer	Procedureel				
		2. de methoden en technieken waarmee wordt vastgesteld dat de ingevoerde maatregelen en procedures voor beveiliging voldoen aan het beveiligingsbeleid van de organisatie;	Beheer	Procedureel				
		3. de frequentie waarmee de controles op handhaving en naleving plaatsvinden;	Beheer	Procedureel				
		4. het aangeven van gebieden waarop specialistisch advies binnen de organisatie noodzakelijk is en de wijze waarop dit specialistisch advies wordt georganiseerd;	Beheer	Procedureel				
		5. de zorg voor een voldoende kennisniveau van het personeel;	Beheer	Procedureel				
		6. de wijze waarop het beleid, het betreffende plan en de te nemen maatregelen ten aanzien van de beveiliging van persoonsgegevens, worden gecommuniceerd naar de medewerkers in de organisatie, de klanten, de leveranciers en overige derden;	Beheer	Procedureel				
		7. de wijze waarop incidenten en inbreuken op de beveiliging van persoonsgegevens worden gemeld en afgehandeld.	Beheer	Procedureel				
7.1.7	1	Bij het opstellen van een implementatieplan voor een bepaalde periode wordt aandacht besteed aan:	Beheer	Procedureel				
		.- het uitvoeren van een analyse voor elke verwerking van persoonsgegevens om te bepalen in welke risicoklasse de persoonsgegevens moeten worden opgenomen;	Beheer	Procedureel				

		.- het tijdspad waarbinnen het plan moet worden uitgevoerd;	Beheer	Procedureel				
		.- het definiëren van de functies en verantwoordelijkheden voor de uitvoering van het plan.	Beheer	Procedureel				
7.1.8	1	De manager onder wiens gedelegeerde verantwoordelijkheid het dagelijkse beheer van de verwerking van persoonsgegevens plaatsvindt, legt de benodigde maatregelen en procedures voor beveiliging van persoonsgegevens vast, implementeert deze en draagt deze uit. Het handhaven respectievelijk naleven van de maatregelen en procedures wordt volgens een van tevoren vastgesteld schema gecontroleerd.	Beheer	Procedureel				
7.1.9	1	De taken van de verantwoordelijk manager omvatten ten minste:	Beheer	Procedureel				
		.- het beschrijven van de maatregelen en procedures voor het beveiligen van de verwerking van persoonsgegevens conform het beveiligingsbeleid en -plan;	Beheer	Procedureel				
		.- het schriftelijk vastleggen van de maatregelen en procedures voor het beveiligen van persoonsgegevens;	Beheer	Procedureel				
		.- het actualiseren van de verantwoordelijkheden, bevoegdheden en taken van de betrokken medewerkers;	Beheer	Procedureel				
		.- een programma ter stimulering van het privacybewustzijn rond het verwerken van persoonsgegevens;	Beheer	Procedureel				
		.- het toezicht houden op de handhaving en naleving van de maatregelen en procedures.	Beheer	Procedureel				
		2. Administratieve organisatie		Procedureel				
7.2.1	1	De richtlijnen met betrekking tot de administratieve organisatie betreffende het beheer van de verwerking van persoonsgegevens worden expliciet vastgelegd.	Beheer	Procedureel				
7.2.2	1	Bij wijzigingen van het stelsel van maatregelen en procedures voor de beveiliging van persoonsgegevens, wordt de beschreven administratieve organisatie overeenkomstig aangepast.	Beheer	Procedureel				
7.2.3	1	De inrichting van de technische maatregelen sluit aan op de organisatorische maatregelen voor de beveiliging van de persoonsgegevens zoals die in het beveiligingsplan zijn weergegeven.	Beheer	Procedureel				
7.2.4	1	De verantwoordelijkheid voor het onderhouden van de beschrijving van de administratieve organisatie wordt expliciet toegewezen.	Beheer	Procedureel				
		3. Beveiligingsbewustzijn						
7.3.1	1	Alle werknemers, inclusief de tijdelijke werknemers, worden geïnstrueerd over het informatiebeleid inzake het beveiligen van persoonsgegevens. Het beleid en de daarbij behorende maatregelen en procedures worden schriftelijk verstrekt of on-line beschikbaar gesteld.	Beheer	Procedureel				
7.3.2	1	De gebruikers nemen kennis van het stelsel van beveiligingsmaatregelen en -procedures op het gebied van de beveiliging van persoonsgegevens en leren op correcte wijze om te gaan met onderdelen van de ICT-infrastructuur waarmee zij in aanraking komen.	Beheer / ontwikkeling	Procedureel				
7.3.3	1	Bij trainingen voor informatiesystemen en beveiligingsmaatregelen op het gebied van de beveiliging van persoonsgegevens worden uitsluitend gegevens van niet- bestaande personen gebruikt.	Beheer	Procedureel				
7.3.4	1	Passende disciplinaire maatregelen worden genomen bij het doorbreken van de geheimhoudingsplicht of het niet correct uitvoeren van de maatregelen en procedures.	Beheer / ontwikkeling	Procedureel				
7.3.5	1	Gedurende functioneringsgesprekken en beoordelingen komt het onderwerp beveiliging van persoonsgegevens aan de orde.	Beheer	Procedureel				
		4. Eisen te stellen aan personeel						
7.4.1	1	Bij de aanstelling tekenen alle medewerkers die met persoonsgegevens zullen gaan werken een geheimhoudingsverklaring. Dit geldt ook voor tijdelijke medewerkers, bijvoorbeeld via hun contract met het uitzendbureau. Bij aanstelling van personeelsleden komen de volgende punten aan bod: .- de controle op de juistheid van het curriculum vitae van de sollicitant door het vragen naar bewijsstukken zoals diploma's en getuigschriften; .- de controle van de identiteit door middel van een legitimatiebewijs. Dit is overigens een algemene verplichting ingevolge de Wet op de identificatieplicht.	Beheer / ontwikkeling	Procedureel				
		5. Inrichting van de werkplek						

7.5.1	1	De verantwoordelijke stelt maatregelen en procedures vast voor het verwerken van persoonsgegevens. Deze moeten schriftelijk worden vastgelegd en bij alle medewerkers bekend zijn. Hierin wordt minimaal het volgende opgenomen: .- de randapparatuur wordt zodanig opgesteld dat deze onder toezicht staat. Voorkomen moet worden dat de apparatuur wordt gebruikt door onbevoegden, dat de uitvoer van de apparatuur door onbevoegden kan worden gelezen of dat anderszins onbevoegd inzage in persoonsgegevens kan worden verkregen; .- de gegevensdragers mogen niet onbeheerd op een onveilige plaats achterblijven (Clean Desk policy); .- de beeldschermen zijn voorzien van een screensaver met wachtwoord waarbij automatisch wordt uitgelogd indien de apparatuur een bepaalde tijd niet gebruikt is.	Beheer	Procedureel				
		6. Beheer en classificatie van de ICT infrastructuur						
7.6.1	1	In het ontwikkelingstraject van informatiesystemen worden de maatregelen en procedures voor de beveiliging van persoonsgegevens en de controle daarop geïnventariseerd, zodat kan worden nagegaan of voldaan wordt aan het informatiebeveiligingsbeleid met betrekking tot de beveiliging van persoonsgegevens. De maatregelen die voortvloeien uit deze inventarisatie moeten bij de ontwikkeling van de software worden geïmplementeerd (onder meer door het toepassen van PET).	Ontwikkeling	Technisch				
7.6.2	1	Bij de ontwikkeling en het onderhoud van informatiesystemen worden toereikende procedures voor changemanagement en versiebeheer gevolgd. De beslissingsbevoegdheid in deze procedures ligt bij de verantwoordelijke voor de persoonsgegevens waarvoor de informatiesystemen worden ontwikkeld, onderhouden of geëxploiteerd.	Beheer / ontwikkeling	Procedureel				
7.6.3	1	Aan documentatie behorende bij de verwerking van persoonsgegevens wordende volgende eisen gesteld: .- de verwerking van persoonsgegevens wordt, indien niet daarvan vrijgesteld, aangemeld bij het CBP of de functionaris voor de gegevensbescherming (artikel 27 tot en met 30, artikel 62 tot en met 64 WBP); .- de volgende onderwerpen worden tenminste gedocumenteerd: datamodellen, software, datacommunicatieprotocollen, alsmede de onderdelen waaruit het proces van de verwerking van de persoonsgegevens bestaat; .- de toegekende (tijdelijke) bevoegdheden in de organisatie worden in een overzicht bijgehouden.	Ontwikkeling	Procedureel				
7.6.4	1	Voor het ondervangen van calamiteiten, incidenten of problemen met betrekking tot de verwerking van persoonsgegevens (binnen het ICT-domein) moeten door of namens de verantwoordelijke goedgekeurde procedures zijn opgesteld. Bij toepassing van deze procedures moeten alle door de gebruiker ondernomen acties worden vastgelegd. Deze vastlegging gebeurt zodanig dat manipulatie van de gegevens niet mogelijk is.	Beheer	Procedureel				
7.6.5	1	Voor het kunnen ondervangen van incidenten met een verwerking van persoonsgegevens, waarbij de ICT-infrastructuur de mogelijke oorzaak kan zijn, is inzicht in het configurationmanagement- systeem noodzakelijk.	Beheer	Procedureel				
		7. Toegangsbeheer en –controle						
7.7.1	1	De verantwoordelijke geeft aan welke functionarissen toegang tot de persoonsgegevens mogen hebben en welke functie(s) mogen worden uitgevoerd. Tevens geeft de verantwoordelijke aan, wie in de organisatie bevoegdheden voor het verwerken van persoonsgegevens mag toedelen. De verantwoordelijke dient hiertoe een procedure vast te stellen. Gewaarborgd is, zowel in de organisatie als in de ICT- infrastructuur, dat de toegekende bevoegdheden volledig en juist in het toegangscontrolesysteem zijn geïmplementeerd. Voor de toegang tot persoonsgegevens worden slechts specifieke toegangsbevoegdheden afgegeven. Een bevoegdheidsprofiel wordt nauwkeurig samengesteld en mag slechts op een zo klein mogelijke verzameling van bevoegdheden betrekking hebben.	Beheer	Procedureel				

7.7.2	1	Aangegeven wordt welke handelingen met welke persoonsgegevens door een functionaris mogen worden uitgevoerd. Bij ontslag, vertrek, wijziging van functie of bij verlies van bevoegdheid om andere redenen, worden de bevoegdheden van de betrokken functionaris met onmiddellijke ingang ontnomen.	Beheer	Procedureel				
7.7.3	1	Voor extern personeel wordt voor het definiëren en toekennen van bevoegdheden een overeenkomstige procedure als voor het eigen personeel toegepast. Deze regel geldt tevens voor opsporingsambtenaren, indien zij in het kader van een justitieel onderzoek toegang verkrijgen tot een verwerking van persoonsgegevens.	Beheer	Procedureel				
7.7.4	1	De opzet van een logische toegangscontrole op informatiesystemen is zodanig dat alleen een functionaliteit kan worden gebruikt waarvoor uitdrukkelijk een bevoegdheid is verleend.	Ontwikkeling	Technisch				
7.7.5	1	Bij de logische toegangscontrole wordt de identiteit en de authenticiteit van gebruikers vastgesteld door ten minste een gebruikersnaam en een wachtwoord.	Ontwikkeling	Technisch				
7.7.6	1	Een wachtwoord is slechts gedurende een van tevoren vastgestelde periode geldig. Bij wijziging van het wachtwoord wordt gecontroleerd of het oude en nieuwe wachtwoord niet gelijk zijn. Voor de hand liggende wachtwoorden zijn niet toegestaan. Tevens moeten er regels opgesteld zijn waarin is vastgelegd aan welke eisen een goed gekozen wachtwoord moet voldoen. Het systeem voor toegangscontrole moet hierop ook controleren.	Ontwikkeling	Technisch				
7.7.7	1	Het wachtwoord wordt nergens in leesbare vorm vastgelegd. In het systeem voor toegangscontrole worden de wachtwoorden voldoende beveiligd, bijvoorbeeld door een one-way-hashing encryptie algoritme.	Ontwikkeling	Technisch				
7.7.8	1	Het aantal keren dat een foutief wachtwoord kan worden ingevoerd, moet worden beperkt tot maximaal drie. Bij overschrijding hiervan wordt de toegang tot het systeem onder de betreffende identificatie volledig geblokkeerd. Slechts een hiertoe geautoriseerde functionaris is gerechtigd de geblokkeerde identificatie weer vrij te geven. Dit gebeurt conform een vastgestelde procedure nadat de afwijkingen zijn onderzocht.	Ontwikkeling	Technisch				
		8. Netwerken en externe verbindingen						
7.8.1	1	De verantwoordelijke legt vast op welke wijze de datacommunicatie plaats behoort te vinden.	Beheer	Procedureel				
7.8.2	1	Er wordt gebruikgemaakt van de beveiligingsopties die de aanwezige netwerkapparatuur en software bieden.	Ontwikkeling	Technisch				
7.8.3	1	Toegang tot en vanuit publiek toegankelijke netwerken zoals internet wordt uitsluitend gemaakt via algemeen erkende beveiligingsmaatregelen, zoals firewalls.	Ontwikkeling	Technisch				
7.8.4	1	Bijzondere aandacht wordt gegeven aan het voorkomen van onbevoegde toegang tot persoonsgegevens via netwerkverbindingen (inbelpunten, modems, etc.).	Ontwikkeling	Technisch				
7.8.5	1	Netwerkfaciliteiten waarmee toegang kan worden verkregen tot persoonsgegevens, moeten verder worden afgeschermd door middel van een logische toegangsbeveiliging.	Ontwikkeling	Technisch				
		9. Gebruik van software						
7.9.1	1	Voor het verwerken van persoonsgegevens wordt gebruikgemaakt van door de verantwoordelijke goedgekeurde software.	Ontwikkeling	Procedureel				
7.9.2	1	Bij aanschaf van software voor de verwerking van persoonsgegevens wordt rekening gehouden met de beveiligingseisen.	Ontwikkeling	Technisch				
7.9.3	1	Er moet een adequate administratie van het versiebeheer van de software worden gevoerd en dit moet worden gedocumenteerd. De procedures voor het onderhoud worden schriftelijk vastgelegd. De wijzigingen worden door de verantwoordelijke goedgekeurd.	Beheer	Procedureel				
		10. Bulkverwerking van gegevens						
7.10.1	1	Het verwerken van persoonsgegevens is alleen toegestaan met een door de verantwoordelijke schriftelijk geautoriseerde versie van de gebruikte software.	Ontwikkeling	Procedureel				
7.10.2	1	Voor de verwerking van persoonsgegevens moet aangegeven zijn welke persoonsgegevens het betreft, met welke software wordt gewerkt, welke bestanden nodig zijn en welke verwerkingen worden uitgevoerd.	Beheer	Procedureel				

7.10.3	1	Voor de afhandeling van calamiteiten tijdens de geautomatiseerde bulkverwerking van persoonsgegevens moeten procedures aanwezig zijn. In voorkomende gevallen worden de oorzaak, de gevolgen en de getroffen maatregelen schriftelijk vastgelegd.	Beheer	Procedureel				
7.10.4	1	De instructies voor de uit te voeren handelingen zijn van tevoren expliciet vastgelegd en goedgekeurd door of namens de verantwoordelijke. Om persoonsgegevens te mogen verwerken moet het personeel daartoe zijn opgeleid.	Beheer	Procedureel				
7.10.5	1	De productieverslagen (logbestanden) van de gegevensverwerkende processen met persoonsgegevens moeten voldoende lang worden bewaard voor bewijs- en analysedoeleinden.	Ontwikkeling	Technisch				
7.10.6	1	Uitsluitend bevoegde personen hebben toegang tot de productieverslagen van persoonsgegevensverwerkende processen.	Beheer	Technisch				
		11. Bewaren van gegevens						
7.11.1	1	De gegevensdragers met persoonsgegevens moeten op een zodanige wijze worden bewaard en behandeld dat alleen bevoegde personen er over kunnen beschikken.	Beheer	Technisch				
7.11.2	1	Er mogen geen gegevensdragers met persoonsgegevens onbeheerd worden achtergelaten op algemeen toegankelijke plaatsen.	Beheer	Technisch				
		12. Vernietigen van gegevens						
7.12.1	1	Het vernietigen van persoonsgegevens nadat de bewaartermijn is verlopen moet zorgvuldig gebeuren. Afdoende maatregelen worden genomen om te voorkomen dat de persoonsgegevens fysiek aanwezig blijven op elektromagnetische gegevensdragers en op eenvoudige wijze weer beschikbaar kunnen worden gemaakt. Persoonsgegevens die op een ander medium zijn vastgelegd (Cd-rom, microfilm, etc.) worden zorgvuldig vernietigd.	Beheer	Technisch				
7.12.2	1	Voor het vernietigen van persoonsgegevens is de toestemming van de verantwoordelijke nodig. De vernietigingsprocedure voor originelen, kopieën, back-ups en andere bestanden dient inzichtelijk te zijn voor de verantwoordelijke. De verantwoordelijke zorgt ervoor dat de procedure en het protocol voor de vernietiging van persoonsgegevens schriftelijk zijn vastgelegd.	Beheer	Procedureel				
7.12.3	1	Aandacht wordt ook besteed aan de vernietiging van tussen- en testresultaten behorende bij de verwerking van persoonsgegevens.	Ontwikkeling	Technisch				
		13. Calamiteitenplan / Continuïteitsplan						
7.13.1	1	Van elk bestand met persoonsgegevens worden een of meerdere back-ups gemaakt. Een exemplaar van de back-up wordt op een andere locatie bewaard dan waar de originele persoonsgegevens zich bevinden.	Beheer	technisch				
7.13.2	1	Voor elke back-up met persoonsgegevens wordt een bewaartermijn vastgesteld.	Beheer	Procedureel				
		14. Uitbesteden van verwerking van persoonsgegevens						
7.14.1	1	In het kader van de controle van de verantwoordelijke op de bewerker kan deze gebruikmaken van een Third Party Mededeling. Dit is een onafhankelijk oordeel over de kwaliteit van de door de bewerker getroffen maatregelen van de beveiliging van persoonsgegevens.	Beheer					
7.14.2	1	In een contract tussen de verantwoordelijke en de bewerker wordt vastgelegd dat beide zich aan de, op de risicoklasse betrekking hebbende, eisen zullen houden. Hierbij wordt onder meer het volgende vastgelegd: .- procedures rond autorisaties; .- het bijhouden van logbestanden; .- de opslag van gegevensdragers met persoonsgegevens; .- het verstrekken van persoonsgegevens aan derden.	Beheer	Procedureel				
7.14.3	1	Het fysieke en logische beveiligingsniveau bij de bewerker moet toereikend zijn voor de risicoklasse van de te verwerken persoonsgegevens.	Beheer	Technisch				
7.14.4	1	De verantwoordelijke dient zich op de hoogte te stellen van het beveiligingsniveau voor de persoonsgegevens bij de bewerker. De verantwoordelijke moet een geheimhoudingsartikel in het contract opnemen.	Beheer	Procedureel				

REF	Maatregel	Fase	Type	Prioriteit	Uitwerking	Verwachtwoordelijke	Inspanning
V.1	Security Architecture Documentation Requirements						
V.1.1	Verify that all application components (either individual or groups of source files, libraries, and/or executables) that are present in the application are identified.	Ontwikkeling	Technisch				
V.1.2	Verify that all components that are not part of the application but that the application relies on to operate are identified.	Ontwikkeling	Technisch				
V.1.3	Verify that a high-level architecture for the application has been defined.	Ontwikkeling	Technisch				
V.2	Authentication Verification Requirements						
V.2.1	Verify that all pages and resources require authentication except those specifically intended to be public.	Ontwikkeling	Technisch				
V.2.2	Verify that all password fields do not echo the user's password when it is entered, and that password fields (or the forms that contain them) have autocomplete disabled.	Ontwikkeling	Technisch				
V.2.3	Verify that if a maximum number of authentication attempts is exceeded, the account is locked for a period of time long enough to deter brute force attacks.	Ontwikkeling	Technisch				
V.2.4	Verify that all authentication controls are enforced on the server side.	Ontwikkeling	Technisch				
V.2.5	Verify that all authentication controls (including libraries that call external authentication services) have a centralized implementation.	Ontwikkeling	Technisch				
V.2.6	Verify that all authentication controls fail securely.	Ontwikkeling	Technisch				
V.2.7	Verify that the strength of any authentication credentials are sufficient to withstand attacks that are typical of the threats in the deployed environment.	Ontwikkeling	Technisch				
V.2.8	Verify that all account management functions are at least as resistant to attack as the primary authentication mechanism.	Ontwikkeling	Technisch				
V.2.9	Verify that users can safely change their credentials using a mechanism that is at least as resistant to attack as the primary authentication mechanism.	Ontwikkeling	Technisch				
V.2.10	Verify that re-authentication is required before any application-specific sensitive operations are permitted.	Ontwikkeling	Technisch				
V.2.11	Verify that after an administratively-configurable period of time, authentication credentials expire.	Ontwikkeling	Technisch				
V.2.12	Verify that all authentication decisions are logged.	Ontwikkeling	Technisch				
V.2.13	Verify that account passwords are salted using a salt that is unique to that account (e.g., internal user ID, account creation) and hashed before storing.	Ontwikkeling	Technisch				
V.2.14	Verify that all authentication credentials for accessing services external to the application are encrypted and stored in a protected location (not in source code).	Ontwikkeling	Technisch				
V.3	Session Management Verification Requirements						
V.3.1	Verify that the framework's default session management control implementation is used by the application.	Ontwikkeling	Technisch				
V.3.2	Verify that sessions are invalidated when the user logs out.	Ontwikkeling	Technisch				
V.3.3	Verify that sessions timeout after a specified period of inactivity.	Ontwikkeling	Technisch				
V.3.5	Verify that all pages that require authentication to access them have logout links.	Ontwikkeling	Technisch				
V.3.6	Verify that the session id is never disclosed other than in cookie headers; particularly in URLs, error messages, or logs. This includes verifying that the application does not support URL rewriting of session cookies.	Ontwikkeling	Technisch				
V.3.7	Verify that the session id is changed on login.	Ontwikkeling	Technisch				
V.3.8	Verify that the session id is changed on reauthentication.	Ontwikkeling	Technisch				
V.3.9	Verify that the session id is changed or cleared on logout.	Ontwikkeling	Technisch				
V.3.10	Verify that only session ids generated by the application framework are recognized as valid by the application.	Ontwikkeling	Technisch				
V.4	Access Control Verification Requirements						

V.4.1	Verify that users can only access protected functions for which they possess specific authorization.	Beheer	Procedureel				
V.4.2	Verify that users can only access URLs for which they possess specific authorization.	Beheer	Procedureel				
V.4.3	Verify that users can only access data files for which they possess specific authorization.	Beheer	Procedureel				
V.4.4	Verify that direct object references are protected, such that only authorized objects are accessible to each user.	Ontwikkeling	Technisch				
V.4.5	Verify that directory browsing is disabled unless deliberately desired.	Beheer	Technisch				
V.4.6	Verify that users can only access services for which they possess specific authorization.	Beheer	Technisch				
V.4.7	Verify that users can only access data for which they possess specific authorization.	Beheer	Procedureel				
V.4.8	Verify that access controls fail securely.	Beheer	Technisch				
V.4.9	Verify that the same access control rules implied by the presentation layer are enforced on the server side.	Beheer	Technisch				
V.4.10	Verify that all user and data attributes and policy information used by access controls cannot be manipulated by end users unless specifically authorized.	Beheer	Procedureel				
V.4.11	Verify that all access controls are enforced on the server side.	Beheer	Technisch				
V.4.12	Verify that there is a centralized mechanism (including libraries that call external authorization services) for protecting access to each type of protected resource.	Ontwikkeling	Technisch				
V.4.13	Verify that limitations on input and access imposed by the business on the application (such as daily transaction limits or sequencing of tasks) cannot be bypassed.	Ontwikkeling	Technisch				
V.4.14	Verify that all access control decisions can be logged and all failed decisions are logged.	Ontwikkeling	Technisch				
V.5	**Input Validation Verification Requirements**						
V.5.1	Verify that the runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.	Ontwikkeling	Technisch				
V.5.2	Verify that a positive validation pattern is defined and applied to all input.	Ontwikkeling	Technisch				
V.5.3	Verify that all input validation failures result in input rejection or input sanitization.	Ontwikkeling	Technisch				
V.5.4	Verify that a character set, such as UTF-8, is specified for all sources of input.	Ontwikkeling	Technisch				
V.5.5	Verify that all input validation is performed on the server side.	Ontwikkeling	Technisch				
V.5.6	Verify that a single input validation control is used by the application for each type of data that is accepted.	Ontwikkeling	Technisch				
V.5.7	Verify that all input validation failures are logged.	Ontwikkeling	Technisch				
V.6	**Output Encoding/Escaping Verification Requirements**						
V.6.1	Verify that all untrusted data that are output to HTML (including HTML elements, HTML attributes, javascript data values, CSS blocks, and URI attributes) are properly escaped for the applicable context.	Ontwikkeling	Technisch				
V.6.2	Verify that all output encoding/escaping controls are implemented on the server side.	Ontwikkeling	Technisch				
V.6.3	Verify that output encoding /escaping controls encode all characters not known to be safe for the intended interpreter.	Ontwikkeling	Technisch				
V.6.4	Verify that all untrusted data that is output to SQL interpreters use parameterized interfaces, prepared statements, or are escaped properly.	Ontwikkeling	Technisch				
V.6.5	Verify that all untrusted data that are output to XML use parameterized interfaces or are escaped properly.	Ontwikkeling	Technisch				
V.6.6	Verify that all untrusted data that are used in LDAP queries are escaped properly.	Ontwikkeling	Technisch				
V.6.7	Verify that all untrusted data that are included in operating system command parameters are escaped properly.	Ontwikkeling	Technisch				
V.6.8	Verify that all untrusted data that are output to any interpreters not specifically listed above are escaped properly.	Ontwikkeling	Technisch				
V.7	**Cryptography Verification Requirements**						

V.7.1	Verify that all cryptographic functions used to protect secrets from the application user are implemented server side.	Ontwikkeling	Technisch				
V.7.2	Verify that all cryptographic modules fail securely.	Ontwikkeling	Technisch				
V.7.3	Verify that access to any master secret(s) is protected from unauthorized access (A master secret is an application credential stored as plaintext on disk that is used to protect access to security configuration information).	Beheer	Technisch				
V.7.4	Verify that password hashes are salted when they are created.	Ontwikkeling	Technisch				
V.7.5	Verify that cryptographic module failures are logged.	Ontwikkeling	Technisch				
V.7.6	Verify that all random numbers, random file names, random GUIDs, and random strings are generated using the cryptographic module's approved random number generator when these random values are intended to be unguessable by an attacker.	Ontwikkeling	Technisch				
V.8	**Error Handling and Logging Verification Requirements**						
V.8.1	Verify that that the application does not output error messages or stack traces containing sensitive data that could assist an attacker, including session id and personal information.	Ontwikkeling	Technisch				
V.8.2	Verify that all server side errors are handled on the server.	Ontwikkeling	Technisch				
V.8.3	Verify that all logging controls are implemented on the server.	Ontwikkeling	Technisch				
V.8.4	Verify that error handling logic in security controls denies access by default.	Ontwikkeling	Technisch				
V.8.5	Verify security logging controls provide the ability to log both success and failure events that are identified as security-relevant.	Ontwikkeling	Technisch				
V.8.6	Verify that each log event includes: 1. a time stamp from a reliable source, 2. severity level of the event, 3. an indication that this is a security relevant event (if mixed with other logs), 4. the identity of the user that caused the event (if there is a user associated with the event), 5. the source IP address of the request associated with the event, 6. whether the event succeeded or failed, and 7. a description of the event.	Ontwikkeling	Technisch				
V.8.7	Verify that all events that include untrusted data will not execute as code in the intended log viewing software.	Ontwikkeling	Technisch				
V.8.8	Verify that security logs are protected from unauthorized access and modification.	Beheer	Technisch				
V.8.9	Verify that there is a single logging implementation that is used by the application.	Ontwikkeling	Technisch				
V.8.10	Verify that that the application does not log application-specific sensitive data that could assist an attacker, including user's session ids and personal or sensitive information.	Ontwikkeling	Technisch				
V.8.11	Verify that a log analysis tool is available which allows the analyst to search for log events based on combinations of search criteria across all fields in the log record format supported by this system.	Beheer	Technisch				
V.9	**Data Protection Verification Requirements**						
V.9.1	Verify that all forms containing sensitive information have disabled client side caching, including autocomplete features.	Ontwikkeling	Technisch				
V.9.2	Verify that the list of sensitive data processed by this application is identified, and that there is an explicit policy for how access to this data must be controlled, and when this data must be encrypted (both at rest and in transit). Verify that this policy is properly enforced.	Beheer	Procedureel				
V.9.3	Verify that all sensitive data is sent to the server in the HTTP message body (i.e., URL parameters are never used to send sensitive data).	Ontwikkeling	Technisch				
V.9.4	Verify that all cached or temporary copies of sensitive data sent to the client are protected from unauthorized access or purged/invalidated after the authorized user accesses the sensitive data (e.g., the proper no-cache and no-store Cache-Control headers are set).	Ontwikkeling	Technisch				
V.9.5	Verify that all cached or temporary copies of sensitive data stored on the server are protected from	Ontwikkeling	Technisch				

V.10	**Communication Security Verification Requirements**						
V.10.1	Verify that a path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and that each server certificate is valid.	Ontwikkeling	Technisch				
V.10.2	Verify that failed TLS connections do not fall back to an insecure connection.	Ontwikkeling	Technisch				
V.10.3	Verify that TLS is used for all connections (including both external and backend connections) that are authenticated or that involve sensitive data or functions.	Ontwikkeling	Technisch				
V.10.4	Verify that backend TLS connection failures are logged.	Beheer	Technisch				
V.10.5	Verify that certificate paths are built and verified for all client certificates using configured trust anchors and revocation information.	Ontwikkeling	Technisch				
V.10.6	Verify that all connections to external systems that involve sensitive information or functions are authenticated.	Ontwikkeling	Technisch				
V.10.7	Verify that all connections to external systems that involve sensitive information or functions use an account that has been set up to have the minimum privileges necessary for the application to function properly.	Ontwikkeling	Technisch				
V.11	**HTTP Security Verification Requirements**						
V.11.1	Verify that redirects do not include unvalidated data.	Ontwikkeling	Technisch				
V.11.2	Verify that the application accepts only a defined set of HTTP request methods, such as GET and POST.	Ontwikkeling	Technisch				
V.11.3	Verify that every HTTP response contains a content type header specifying a safe character set (e.g., UTF-8).	Ontwikkeling	Technisch				
V.11.4	Verify that the HTTPOnly flag is used on all cookies that do not specifically require access from JavaScript.	Ontwikkeling	Technisch				
V.11.5	Verify that the secure flag is used on all cookies that contain sensitive data, including the session cookie.	Ontwikkeling	Technisch				
V.11.6	Verify that HTTP headers in both requests and responses contain only printable ASCII characters.	Ontwikkeling	Technisch				
V.12	**Security Configuration Verification Requirements**						
V.12.1	Verify that all security-relevant configuration information is stored in locations that are protected from unauthorized access.	Beheer	Technisch				
V.12.2	Verify that all access to the application is denied if the application cannot access its security configuration information.	Ontwikkeling	Technisch				