TWINNTAX - Organisatorische en technische maatregelen

	MAATREGELEN
1. Bewustmaking gebruikers	Sessie om de medewerkers te informeren en bewust te maken.
	IT-handvest
	Vertrouwelijkheidsclausule in de arbeidsovereenkomst van de medewerkers
2. Authenticatie gebruikers	Uniek gebruikers-ID en verbod op gedeelde accounts
	Authenticatie van de gebruikers op basis van wachtwoorden
	Beperking van het aantal aanmeldpogingen voor een account
	Beveiligde opslag van wachtwoorden (versleuteling)
3. Beheer bevoegdheden	Aanmaak specifieke bevoegdheidsprofielen voor de systemen (toegang tot bepaalde dossiers)
	Goedkeuring vereist voor elke bevoegdheidsaanvraag
	Verwijdering van toegangsrechten (ook op het einde van een contract)
	Regelmatige (jaarlijkse) controle van de bevoegdheden
4. Tracering activiteiten en incidentbeheer	Logboeksysteem (opslag van logbestanden of 'logs') voor activiteiten van de gebruikers, technische interventies en afwijkingen
	Opslag logbestanden gedurende zes maanden tot een jaar
5. Beveiliging werkposten	Systeem voor automatische vergrendeling sessie vanaf een bepaalde afwezigheidsduur
	Firewall voor elke werkpost
	Regelmatige updates van antivirus- en andere software
	Software instellen om automatische updates door te voeren
	Opslag van gebruikersgegevens op locatie met regelmatige back-ups in plaats van op de werkposten
	Beveiligde verwijdering van werkpostgegevens vooraleer apparatuur wordt toegekend aan een andere persoon
	Verbod op het uitvoeren van toepassingen die niet afkomstig zijn van veilige bronnen
6. Beveiliging mobiele apparatuur	Bewustmaking over risico's zoals diefstal, verbinding met onveilige openbare netwerken ...
	Wachtwoord op mobiele telefoons
	Regelmatige back-ups of synchronisaties

7. Bescherming intern IT-netwerk	Beperking van internettoegang door niet-essentiële diensten te blokkeren (VoIP, peer to peer)
	Beheer en beveiliging van de wifinetwerken (WPA3- of WAP2-versleuteling)
	VPN voor toegang op afstand met mobiele apparaten
8. Beveiliging servers	Toegang tot beheertools en -interfaces uitsluitend voorbehouden voor bevoegde personen
	Kritieke updates meteen installeren
	Gebruik van regelmatig bijgewerkte detectie- en verwijderingssoftware tegen malware
	Back-ups maken
	Implementatie van TLS-protocol (ter vervanging van SSL)
9. Beveiliging websites	Implementatie van TLS-protocol (ter vervanging van SSL) + verplicht maken voor alle authenticatiepagina's
	Beperking van communicatiepoorten tot het strikte minimum voor de goede werking van de geïnstalleerde toepassingen
	Toegang tot beheertools en -interfaces uitsluitend voorbehouden voor bevoegde personen
10. Back-ups en bedrijfscontinuïteit	Regelmatige back-ups van de gegevens
	Opslag van minstens één back-up op een externe locatie
	Opslag van minstens één back-up offline
	Identiek gegevensbeschermingsniveau voor back-ups en gegevens op servers
11. Archivering	Uitwerken van een beheerproces voor de archieven
12. IT-ontwikkelingsactiviteiten	Implementatie van een doeltreffende verdediging voor de systemen (combinatie van verschillende beveiligingsmaatregelen)
	Uitgebreide tests voordat een product ter beschikking wordt gesteld of bijgewerkt
	Audit of codeanalyse vooraleer updates worden doorgevoerd om mogelijke inbreuken op de privacywetgeving te vermijden
13. Beheer onderaanneming	Uitsluitend gebruikmaken van onderaannemers die voldoende waarborgen bieden + een contract voorzien
	Middelen om de waarborgen van de onderaannemer te controleren inzake gegevensbescherming (bv. beveiligingsaudits, bezoek ter plaatse)

14. Beveiliging communicatie met andere instanties	Bij verzendingen via een netwerk: - gevoelige stukken versleutelen - protocol gebruiken dat de vertrouwelijkheid verzekert + authenticatie van doelserver voor bestandsoverdracht, bv. SFTP of HTTPS - vertrouwelijkheid van geheimen garanderen (bv.: codeersleutel, wachtwoord) door ze via een ander kanaal te versturen dan de beschermde gegevens.
15. Bescherming kantoren	Plaatsing alarmsystemen en regelmatige controle goede werking
	Plaatsing rookdetectors en brandbestrijdingssystemen + jaarlijkse inspectie
	Beveiliging van de sleutels van de kantoren en de codes van de alarmsystemen