BBN-score maatregel	BIO-Nummer	Beschrijving maatregel	M4PGOOD	Extra info	
	Overheidsmaatregel				
2+	7.1.1.2	Een **VOG** is de verantwoordelijkheid voor elke dienstenaanbieder/leverancier. Dit opnemen in de afspraken.	mens		
2+	9.2.3.2	Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.	programmatuur		
2+	9.4.1.4	Het aantal sessies dat één gebruiker gelijktijdig kan hebben, is beperkt tot één en wordt gemonitord op misbruik. Maak bij het aanmelden een nieuwe sessie aan en verbreek een eventueel al bestaande sessie van die gebruiker. Maak de oude sessie-identifier ongeldig.	apparatuur	Denk ook aan de mogelijkheid tot inzet van AzureAd i.c.m. Conditional Access van de gemeente Lelystad	
2+	9.4.1.5	Deactiveer of verwijder (deinstallatie) alle functies, protocollen, services en accounts op het ICT-component als die niet noodzakelijk zijn. Toets periodiek (eventueel automatisch) of de in productie zijnde ICT-componenten niet meer dan de vastgestelde noodzakelijke functies bieden (statusopname) en de geconstateerde afwijkingen worden hersteld.	apparatuur		
2+	9.4.3.9	Inactieve accounts worden na 60 dagen geblokkeerd.	programmatuur		
2+	10.1.1.4	Een token (bijvoorbeeld SMS-code / authenticator-code) wordt geblokkeerd indien de code of het wachtwoord **vijf** keer verkeerd wordt ingevoerd.	programmatuur	Denk ook aan de mogelijkheid tot inzet AzureAd van de gemeente Lelystad	
2+	11.2.9.6	Na een periode van inactiviteit **in de applicatie** wordt een sessie uiterlijk na 15 minuten vergrendeld waarbij alle informatie op het beeldscherm onleesbaar en ontoegankelijk wordt.	programmatuur		
2+	12.3.1.9	Back-ups worden zodanig opgeslagen dat bij een incident niet zowel het ICT-systeem als de back-ups worden getroffen	omgeving		
2+	12.4.1.9	ICT-systemen leggen ten minste het volgende vast: • authenticatiegebeurtenissen; • bestands- en objectgebeurtenissen; • export- (bijv. uploads) en importgebeurtenissen (bijv. downloads); • gebeurtenissen betreffende gebruikersaccounts; • gebeurtenissen betreffende accounts met speciale bevoegdheden.	programmatuur		
2+	12.4.1.10	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en over de bevindingen gerapporteerd. Om dit uit te kunnen voeren zijn onderstaande voorwaarde ingevuld: 1) De verschillende gelogde informatie wordt samengebracht voor analysedoeleinden. 2) De signaleringssystemen (detectie) maken tijdig melding van ongewenste gebeurtenissen (alarmeringen). 3) Er zijn procedures vastgelegd met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn. 4) Er is vastgelegd waar en hoe correlaties worden aangebracht (analyseren / auditing). 5) De geregistreerde menselijke en systeemacties worden periodiek geanalyseerd. 6) De ongebruikelijke situaties (incidenten) worden periodiek geanalyseerd. 7) De geanalyseerde en beoordeelde gelogde gegevens worden geconsolideerd en gerapporteerd naar het hoogste management.	organisatie		
2+	12.4.2.7	Offline gearchiveerde logbestanden zijn niet benaderbaar vanaf het ICT-systeem waarop ze gegenereerd zijn.	apparatuur		
2+	12.6.1.2	Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is (kritieke beveiligings-updates/patches) worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten binnen vier weken na beschikbaar komen worden doorgevoerd. Als de inschatting is dat overige applicaties niet meer kunnen werken mag hier vanaf geweken worden, er moet dan wel een workaround bedacht worden. Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van de Informatiebeveiligingsdienst voor gemeenten (IBD).	organisatie		
2+	12.6.1.3	Er mag alleen gebruik worden gemaakt van ICT-systemen (zowel soft- als hardware) die door de leverancier actief worden ondersteund, door het aanbieden van beveiligings-updates/patches. (Zowel voor de eindgebruiker alsook bij de leverancier). Het gaat hier om ICT-systemen die niet het einde van hun levenscyclus (End-of-life) hebben bereikt. Deze ICT systemen dienen voordat de ondersteuning stopt te worden vervangen.	programmatuur		
2+	13.1.2.10	De beveiligingsarchitectuur van ICT-netwerken volgt het principe van minimalisatie: “deny by default and allow by necessity“.	apparatuur	Backoffice op Gemnet?	
2+	13.1.2.22	Het beheer van accounts met verhoogde (of bijzondere) rechten worden continu gemonitord zodat ongeautoriseerde wijzigingen worden gedetecteerd,	mens		
2+	14.1.1.3	De hardening van ICT-componenten wordt actueel gehouden (maak dit onderdeel van wijzigingsbeheer).	programmatuur		
2+	14.1.1.9	De dienstenleverancier en/of de ICT-afdeling zoekt continu naar nieuwe kwetsbaarheden en dreigingen en rapporteert deze aan de lijnmanager en initieert het wijzigingsproces.	organisatie		
2	14.2.1.1	De gangbare principes rondom Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen	diensten		
2+	14.2.7.2	De organisatie controleert (log)bestanden met diagnostische gegevens op de gevoeligheid van deze gegevens alvorens deze naar externe partijen te sturen.	apparatuur		
2+	15.1.2.9	Op basis van de informatiebeveiligingseisen uit de offerteaanvraag / Programma van Eisen (PvE) worden maatregelen expliciet opgenomen in de (inkoop)contracten.	diensten		
2+	15.1.2.10	De BBN2+ infrastructuur maakt uitsluitend gebruik van geëvalueerde en goedgekeurde producten (hardware/software) die de beveiliging waarborgen.	diensten		
2+	15.1.3.3	De BBN2+ infrastructuur wordt gedurende de looptijd van het contract adequaat beschermd.	diensten	Backoffice op Gemnet?	
2+	16.1.2.9	Bij vermoeden van opzet bij compromittering van BBN2+ informatie, wordt onverwijld melding gedaan door de CISO bij de portefeuillehouder voor informatiebeveiliging.	organisatie		
2+	16.1.2.11	Systemen voor continue bewaking (IDS/IPS) geven automatisch een veiligheidswaarschuwing af om het beveiligingspersoneel te waarschuwen.	organisatie		
2+	18.2.2.6	Noodzakelijke afwijkingen van de BIO (O-maatregelen) zijn uitsluitend toegestaan indien de GS hiervoor toestemming heeft verleend. (GS kan deze taak uiteraard mandateren.) Deze toestemming wordt verleend uitsluitend nadat een formele risicoafweging heeft aangetoond dat (bijvoorbeeld met vervangende maatregelen) het beveiligingsrisico als gevolg van de niet-naleving niet is toegenomen. Deze afwijking wordt gedocumenteerd en wordt periodiek gereviewd of het nog nodig is en of er aanvullende maatregelen nodig zijn om de risico's te verminderen.	organisatie		
2+	18.2.3.3	BBN2+ informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen, de fysieke toegang en risico’s ten aanzien van de feitelijke veiligheid. Dit kan bijv. door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.	organisatie		
2+	11.2.1.7	Figuur 1 uit de IBD-handreiking "Afvoer ICT middelen" wordt gehanteerd bij de afvoer van apparatuur die ooit is gebruikt voor de opslag of verwerking van BBN2+ informatie (eigen apparatuur, apparatuur van dienstenleveranciers maar ook laptops van consultant of gehuurde ICT-middelen). https://www.informatiebeveiligingsdienst.nl/product/afvoer-ict-middelen/	apparatuur		
2+	11.2.1.8	Externe medewerkers en ingehuurd personeel werken met BBN2+ informatie uitsluitend op door de gemeente verstrekte apparatuur.	apparatuur	Denk ook aan de mogelijkheid tot inzet van AzureAd i.c.m. Conditional Access van de gemeente Lelystad	