	Risico	Prioriteit (1=laag; 2=middel; 3=hoog)	Beheersmaatregelen	Acties	Actie-eigenaar	Deadline
OPSLAG EN VERNIETIGING GEGEVENS	Aangezien alle directies met M365 gaan werken, komen er veel documenten met verschillende (persoons)gegevens in M365 te staan. Als het bewaren en vernietigen niet is ingeregeld, is er sprake van overtreding van artikel 5 AVG.		5.1.2i	5.1.2i	5.1.2e	Q3 2022
	Medewerkers weten niet waar informatie moet worden opgeslagen waardoor PNH deze kwijt kan raken.				5.1.2e 5.1.2e	
	Ontbreken van workflow in de huidige SharePoint omgevingen.				5.1.2e	
BEVEILIGING	Aangezien alle directies met M365 gaan werken, komen er veel documenten met verschillende (persoons)gegevens in M365 te staan. Deze documenten dienen op adequate wijze beschemrd te worden. Directies moeten weten hoe en welke classificatie zij moeten meegeven aan het betreffende document.				5.1.2e 5.1.2e	Q3 2022
	Statenleden mogen via M365 geen toegang hebben tot documenten van gedeputeerde staten. Als dat wel het geval is, is er waarschijnlijk sprake van een datalek				5.1.2e	Voor staten verkiezingen 2023
	Er dient ook een back up aanwezig te zijn voor het geval we gehackt worden/ ransomeware				Stuurgroep Digitaal samenwerken	Q3 2022
	Eigenaarschap en Operationeel beheer van de Security functionaliteiten ontbreekt				5.1.2e	z.s.m.
SAMENWERKEN/ DELEN VAN INFORMATIE	Er kan met externen worden samengwerkt in documenten op M365. Hierdoor bestaat het riscico dat externen minder zorgvuldig zullen omgaan met deze (persoonsgegevens).				5.1.2e	Q3 2022
Compliance	Eigenaarschap en Operationele beheer van de compliance functionaliteiten ontbreekt				5.1.2e (MT-CID)	z.s.m.

Privacyprotocol ICT-middelengebruik

HOOFDSTUK 1 ALGEMENE BEPALINGEN

ARTIKEL 1.1 OVERWEGINGEN

1. Overwegende dat:
   a. de provincie Noord-Holland aan personeelsleden ICT-middelen ter beschikking stelt om met behulp daarvan hun functie uit te oefenen;
   b. het gewenst is voor alle gebruikers duidelijke regels voor inzicht in het gebruik van die ICT-Middelen vast te leggen;
   c. het gewenst is een specifiek privacyprotocol inzake ICT-middelengebruik vast te stellen waarin regels zijn opgenomen voor het registreren, monitoren en controleren van dit gebruik van de ICT-middelen;
2. Het protocol is vastgesteld gelet op:
   a. de Algemene verordening gegevensbescherming, nr. 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (AVG) en
   b. de Uitvoeringswet Algemene verordening gegevensbescherming.

ARTIKEL 1.2 DEFINITIES

In dit protocol wordt verstaan onder:

a. account: digitale identiteit, uniek gekoppeld aan een personeelslid, waaraan rechten, authenticatie en de logging wordt gekoppeld;
b. Algemeen privacyreglement: het Algemeen privacyreglement persoonsgegevens van personeelsleden;
c. AVG: Algemene verordening gegevensbescherming, nr. 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens;
d. beheerder: de ambtenaar of ingehuurde die belast is met het beheer van de provinciale ICT-infrastructuur of een onderdeel daarvan;
e. besluit: Besluit mandaat, volmacht- en machtiging Human Resource Management;
f. betrokkene: degene op wie een persoonsgegeven betrekking heeft, in dit geval personeelsleden en andere natuurlijke personen;
g. directeur: de directeur van het betrokken personeelslid;
h. eigenaar: de verantwoordelijke van informatieverwerkingen, waaronder het beheer en de toegangsverlening;
i. FG: de functionaris gegevensbescherming zoals genoemd in de AVG;
j. gebruik: het gebruik van de ICT-middelen;
k. ICT-middelen: de door of namens de provincie aan personeelsleden ter ondersteuning van de functie-uitoefening van de personeelsleden ter beschikking gestelde ICT-middelen, waaronder:
   a. e-mailfaciliteiten, zoals het e-mailadres, de mailbox en toegang tot de faciliteiten van buiten de provincie;
   b. internet- en andere netwerkfaciliteiten: internet-toegang, waaronder ook via GSM 4G en Wifi;
   c. telefoniefaciliteiten, zoals telefoonnummers, doorschakelfaciliteiten, voicemail;
   d. ICT-apparatuur, waaronder alle huidige en toekomstige elektronische communicatie- en informatieapparatuur en software, zoals telefoon, tablet en laptop. Onderliggend omvat dit de werkplek- en bedrijfsapplicaties met alle functionele autorisaties en transactievastlegging;
l. incident: (het vermoeden van) gepleegde of te plegen strafbare feiten, dan wel handelingen die in strijd zijn met de afgelegde eed of belofte, met de provinciale gedragscode of met de integriteitsverklaring voor externen – welke vermoedelijk met behulp van ICT-middelen hebben plaatsgevonden;
m. leidinggevende: de formeel leidinggevende van het betrokken personeelslid;
n. logging: vastlegging van gebeurtenissen in de ICT-middelen, onder andere gebeurtenissen die voortvloeien uit het gebruik van deze middelen door wie en wanneer (niet de inhoud);
o. monitoring: het doorlopend, (of steekproefsgewijs) en incidenteel inzien van logging door beheerders;

p. observatie: het onderzoeken van het gebruik van ICT-middelen door kennis te nemen van de beschikbare inhoud van elektronische postbussen, het mobiel- en internetverkeer, de toegang tot de laptop;
q. personeelslid: de persoon in dienst van de provincie of de persoon die werkzaam is bij de provincie of voor de provincie werkzaam is geweest;
r. persoonsgegevens: alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd;
s. PIA: Data Protection Impact Assessment;
t. protocol: het Privacyprotocol ICT-Middelengebruik;
u. provincie: de provincie Noord-Holland;
v. verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens, zoals bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, of aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

ARTIKEL 1.3 REIKWIJDTE

1. Dit protocol ziet toe op de verwerking van persoonsgegevens van personeelsleden met betrekking tot het gebruik van ICT-middelen.
2. Dit protocol beschrijft wanneer en op welke wijze de provincie deze gegevens mag inzien. Het beschrijft de toepassing van de bevoegdheden van de provincie.
3. Dit protocol is van toepassing op bij de provincie werkzame personen die gebruik maken van de door de provincie beschikbaar gestelde ICT-middelen.
4. Dit protocol is van toepassing op niet bij de provincie werkzame personen, voor zover er aan deze personen door de provincie toestemming is verleend om gebruik te maken van de door de provincie beschikbaar gestelde ICT-middelen.

ARTIKEL1.4 DOEL

Het doel van de controle op het gebruik door de provincie is om (vermoedelijke) incidenten te onderzoeken en te beoordelen, de aard en omvang van dergelijke incidenten vast te stellen en incidenten te voorkomen respectievelijk ertegen op te treden.

HOOFDSTUK 2 VERWERKING VAN PERSOONSGEGEVENS

ARTIKEL 2.1 VERZAMELING PERSOONSGEGEVENS

1. Logging bevat mogelijk informatie die direct of indirect tot personeelsleden herleidbaar is. De registratie van logging is gebaseerd op technische, kortstondige monitoring en niet op vastlegging van persoonsgegevens. In sommige situaties zijn de gegevens te herleiden naar personen.
2. De provincie legt over het gebruik informatie vast op de grondslag van haar gerechtvaardigd belang om de veiligheid, waaronder beschikbaarheid, integriteit en vertrouwelijkheid, en gebruik van deze ICT-middelen en informatie te waarborgen.
3. De vastlegging beperkt zich tot de gegevens die noodzakelijk zijn voor het doel, genoemd in artikel 1.4.
4. De registratie voor uitgifte van ICT-middelen heeft als primair doel het beheer van ICT-middelen en betreft globaal de volgende persoonsgegevens:
   a. personeelsnummer;
   b. naam, voornaam of voorletters;
   c. directie en sector waar het personeelslid onder valt;
   d. functietitel;
   e. alle identificerende informatie in samenhang met het gebruikte middel, waaronder het telefoonnummer, Simkaart, apparaat-ID, IP- en MAC-adres.

ARTIKEL 2.2 TOEGANG TOT, INZAGE IN EN VERSTREKKING VAN LOGGING EN ANDERE PERSOONSGEGEVENS

1. De eigenaar heeft toegang tot logging. De beheerder heeft toegang tot logging, indien de eigenaar toestemming heeft gegeven. De eigenaar is de eerstverantwoordelijke.
2. De initiële verstrekking van enkel logging in het kader van een onderzoek als bedoeld in artikel 2.3 wordt gedaan door de beheerder(s) aan de leidinggevende.

3. Toegang door middel van observatie geschiedt na een verzoek door de sectormanager van de sector Informatievoorziening & ICT bij de relevante leverancier.
4. Indien er in een onderzoek als bedoeld in artikel 2.4 sprake is van inzage m.b.t. zowel logging als observatie of van een voornemen daartoe, blijft de inzage en toegang – in afwijking van het tweede en derde lid van dit artikel - beperkt tot de sectormanager van de sector Informatievoorziening & ICT.
5. Verstrekking van en inzage in logging over het personeelslid is beperkt tot gevallen waarin sprake is van een (redelijk vermoeden van een) incident, waarbij een onderzoek als bedoeld in artikel 2.3 wordt gestart.
6. Verstrekking van en inzage in persoonsgegevens middels observatie is beperkt tot gevallen waarin sprake is van een incident waarbij niet volstaan kan worden met een onderzoek als bedoeld in artikel 2.3.
7. In geval van monitoring wordt door de beheerder van het ICT-middel een check op de logging gedaan ten behoeve van de beschikbaarheid, integriteit en vertrouwelijkheid van het door het middel ondersteunde proces. De beheerder zal kennisname van persoonsgegevens zoveel mogelijk vermijden en over de monitoring uitsluitend geaggregeerde informatie verspreiden.
8. Er wordt een logboek bijgehouden:
   a. door de beheerder bij verstrekking van logging vanwege een onderzoek als bedoeld in artikel 2.3;
   b. door de beheerder bij monitoring als bedoeld in lid 7;
   c. onder verantwoordelijkheid van de sectormanager Informatievoorziening & ICT in geval van verstrekking van en inzage in logging en/of in geval van observatie.
9. In het logboek wordt in geanonimiseerde vorm beschreven:
   a. het soort incident dat de verstrekking van en/of inzage in logging en/of observatie noodzakelijk heeft gemaakt en
   b. de voor kennisdeling relevante informatie uit de monitoring.
10. Het logboek bevindt zich bij en valt onder verantwoordelijkheid van de sectormanager Informatievoorziening & ICT.
11. De FG heeft te allen tijde toegang tot het logboek.

ARTIKEL 2.3 ONDERZOEK EN INLICHTING PERSONEELSLID BIJ LOGGING

1. De leidinggevende legt een onderzoeksdossier aan, indien er sprake is van een onderzoek naar een incident of een melding daarvan.
2. De leidinggevende informeert de directeur, indien er sprake is van een voldoende gerechtvaardigd belang in de vorm van een redelijk vermoeden van een incident.
3. De leidinggevende start vervolgens nader onderzoek in opdracht van de directeur.
4. Indien in dat geval inzage in logging noodzakelijk is, verricht de beheerder samen met de leidinggevende het nadere onderzoek conform lid 5 en verder.
   Voordat verstrekking van/inzage in logging plaatsvindt, wordt het betrokken personeelslid hierover, over de mogelijke vervolgstappen en de functietitels van de personen die daarbij betrokken zullen zijn schriftelijke geïnformeerd door de leidinggevende.
5. Voordat inzage als bedoeld in lid 4 plaatsvindt, verzoekt de leidinggevende al dan niet samen met de beheerder de FG om advies.
6. Bij het adviesverzoek wordt een schriftelijke onderbouwing van de noodzaak tot inzage verstrekt, indien mogelijk met onderbouwende stukken. De naam van het personeelslid en andere direct identificerende elementen worden geanonimiseerd in het verzoek, de onderbouwing en de overige stukken.
7. Zodra het advies van de FG is ontvangen, vraagt de leidinggevende de algemeen directeur om toestemming onder toezending van het oorspronkelijke adviesverzoek, de daarbij behorende stukken en het advies van de FG. Het advies van de FG is een zwaarwegend advies, waarvan de algemeen directeur gemotiveerd kan afwijken.
8. Indien de algemeen directeur geen toestemming geeft, sluit de leidinggevende het onderzoeksdossier. De leidinggevende verwijdert het dossier 6 maanden na sluiting van het onderzoek. Deze termijn vangt aan op het moment waarop bekend wordt dat geen toestemming wordt verleend. Het personeelslid wordt hierover geïnformeerd door de leidinggevende.
9. Wanneer de toestemming van de algemeen directeur is ontvangen, kan inzage in logging plaatsvinden. De leidinggevende informeert hierna de directeur en verstrekt een verslag van de inzage en de verzamelde logging. Deze stukken maken onderdeel uit van het onderzoeksdossier.

10. De inzage in logging is beperkt tot de tijdspanne waarbinnen het incident, dan wel daarmee verband houdende handelingen, vermoedelijk hebben plaatsgevonden.
11. Na de inzage in de logging vindt een gesprek plaats over het incident tussen de directeur, de leidinggevende en het personeelslid. Hierbij ontvangt het personeelslid van de directeur een kopie van het schriftelijke verslag van de inzage. Waarbij het personeelslid geïnformeerd wordt over de mogelijkheid om binnen zes weken na dagtekening mondeling en/of schriftelijk bij de directeur te reageren op het verslag.
12. Afhankelijk van het onderzoeksdossier en de mogelijke reactie van het personeelslid:
    a. Is er sprake van opheldering en décharge. De leidinggevende stelt het personeelslid hiervan schriftelijk op de hoogte. De eigenaar sluit het onderzoeksdossier en vernietigt dit 6 maanden na sluiting van het onderzoek. Deze termijn vangt aan op het moment van de gerelateerde kennisgeving aan het personeelslid.
    b. Wordt het incident bevestigd en vindt een gesprek plaats tussen het personeelslid en de volgens het besluit aangewezen functionaris over het incident. Hierna wordt door de aangewezen functionaris een beslissing genomen, waarbij afhankelijk van de omstandigheden van het geval een disciplinaire maatregel kan worden opgelegd. De beslissing hiertoe wordt opgenomen in het personeelsdossier. Het onderzoeksdossier wordt gedurende 1 jaar bewaard door de eigenaar, waarna de eigenaar het dossier vernietigt.
13. Bij sluiting van het onderzoeksdossier worden alle gerelateerde correspondentie, documenten en overige gegevens uit de eigen bestanden verwijderd door de bij het onderzoek betrokken personen. De (verrijkte) logging wordt door de eigenaar versleuteld of anderszins effectief beveiligd tegen onbevoegde kennisname. De eigenaar ziet erop toe dat de verwijdering plaatsvindt.

ARTIKEL 2.4 ONDERZOEK EN INLICHTING PERSONEELSLID BIJ OBSERVATIE

1. In gevallen waarin observatie van het gebruik van een personeelslid aan de orde is, én dus geen sprake is van een onderzoek als bedoeld in artikel 2.3 dan wel waarin een onderzoek als bedoeld in artikel 2.3 onvoldoende en/of ongeschikt blijkt te zijn, geldt het bepaalde in dit artikel.
2. Voordat observatie plaatsvindt:
    a. onderbouwt de leidinggevende het incident schriftelijk, is er sprake van een gerechtvaardigd belang en is er een noodzaak waardoor observatie gerechtvaardigd is, waardoor niet kan worden volstaan met een onderzoek als bedoeld in artikel 2.3. De leidinggevende neemt dit op in het onderzoeksdossier en informeert de directeur. De leidinggevende start vervolgens in opdracht van de directeur met nader onderzoek;
    b. dient een PIA te worden uitgevoerd;
    c. wordt het personeelslid hierover, over de mogelijke vervolgstappen en de functietitels van de personen die daarbij betrokken zullen zijn schriftelijk door de leidinggevende geïnformeerd, tenzij gegronde vrees bestaat dat dit nadelig zal zijn voor de bewijsvergaring. In dat geval zal het personeelslid na de observatie worden geïnformeerd conform lid 8;
    d. vraagt de leidinggevende al dan niet samen met de sectormanager van de sector Informatievoorziening & ICT- de Coördinator Integriteit en de FG om advies voor wat betreft de toepassing van observatie en de grenzen daarvan. Bij het adviesverzoek wordt een schriftelijke onderbouwing van de noodzaak tot observatie verstrekt, indien mogelijk met onderbouwende stukken. Hierbij wordt de naam van het personeelslid, en andere direct identificerende elementen, geanonimiseerd in het verzoek, de onderbouwing en de overige stukken;
    e. wordt de algemeen directeur om toestemming gevraagd, onder toezending van het adviesverzoek en de bijbehorende stukken, waaronder het afgegeven advies. Het advies is zwaarwegend, maar de algemeen directeur kan hier gemotiveerd van afwijken.
3. Observatie vindt plaats met toestemming van de algemeen directeur. Indien de algemeen directeur geen toestemming geeft, sluit de leidinggevende het onderzoeksdossier. De leidinggevende verwijdert het dossier 6 maanden na sluiting van het onderzoek. Deze termijn vangt aan op het moment waarop bekend wordt dat geen toestemming wordt verleend. Het personeelslid wordt hierover geïnformeerd door de leidinggevende.

4. Wanneer de toestemming van de algemeen directeur is ontvangen, kan observatie plaatsvinden. De leidinggevende informeert hierna de directeur en verstrekt een verslag van de observatie. Dit verslag maakt onderdeel uit van het onderzoeksdossier.
5. De observatie dient proportioneel en ter zake dienend zijn. Van een personeelslid met een vertrouwensfunctie (de Coördinator Integriteit, leden van de Ondernemingsraad en de vertrouwenspersonen) wordt inhoud van berichten of verkeer niet ingezien, tenzij aangetoond is dat het berichten en/of verkeer betreft die geen verband houden met de vertrouwensfunctie.
6. De observatie is beperkt tot de tijdspanne waarbinnen het incident dan wel daarmee verband houdende handelingen vermoedelijk hebben plaatsgevonden.
7. De algemeen directeur kan de reeds verzamelde gegevens laten samenbrengen en/of combineren met andere persoonsgegevens. Hiertoe dient de leidinggevende een apart verzoek in bij de algemeen directeur. De uitkomst maakt onderdeel uit van het onderzoeksdossier. Indien er sprake is geweest van een onderzoek als bedoeld in artikel 2.3, zullen de in dat kader verzamelde gegevens (waaronder de logging) tevens onderdeel uitmaken van het onderzoeksdossier.
8. Na de observatie vindt een gesprek plaats over het incident tussen de directeur, de leidinggevende en het personeelslid. Hierbij ontvangt het personeelslid van de directeur een kopie van het schriftelijke verslag van de observatie. Waarbij het personeelslid wordt geïnformeerd over de mogelijkheid om binnen zes weken na dagtekening mondeling en/of schriftelijk bij de directeur te reageren op het verslag.
9. Afhankelijk van de uitkomst van de observatie, het verdere onderzoeksdossier en de mogelijke reactie van het personeelslid:
    a. Kan de directeur besluiten dat sprake is van opheldering en décharge. De leidinggevende sluit het onderzoeksdossier vernietigt dit 6 maanden na sluiting van het onderzoek. Deze termijn vangt aan op het moment van de gerelateerde kennisgeving aan het personeelslid;
    b. Wordt het incident bevestigd en vindt een gesprek plaats met het personeelslid en de volgens het besluit aangewezen functionaris over het incident. Hierna wordt door de aangewezen functionaris een beslissing genomen. Waarna afhankelijk van de omstandigheden van het geval een disciplinaire maatregel wordt opgelegd. De beslissing hiertoe wordt opgenomen in het personeelsdossier. Het onderzoeksdossier wordt gedurende 1 jaar bewaard door de eigenaar, waarna de eigenaar het dossier vernietigt.
10. Bij sluiting van het onderzoeksdossier worden alle gerelateerde correspondentie, documenten en overige gegevens door de bij het onderzoek betrokken personen verwijderd uit de bestanden. De (verrijkte) logging en gegevens verkregen uit observatie worden door de eigenaar versleuteld of anderszins effectief beveiligd tegen onbevoegde kennisname. De eigenaar ziet erop toe dat de verwijdering plaatsvindt.

HOOFDSTUK 3 OVERIGE BEPALINGEN

ARTIKEL 3.1 AANVULLENDE BEWAARTERMIJN BIJ OBSERVATIE

In aanvulling op artikel 2.3 worden logging en overige persoonsgegevens uit het onderzoek, bedoeld in artikel 2.4, apart van de algemene logging bewaard. Deze gegevens worden verwijderd zodra het onderzoek is afgerond en er geen procedures van het personeelslid meer lopen. Het personeelslid wordt hiervan op de hoogte gesteld.

ARTIKEL 3.2 TOEZICHT, BEHEER EN BEVEILIGING

1. De beveiliging van informatiemiddelen is in de provincie onderworpen aan kaders vastgelegd in de Baseline Informatiebeveiliging Overheid en het informatiebeveiligingsbeleid van de provincie dat de verantwoordelijkheden en het toezicht op de informatiebeveiliging regelt.
2. De classificatie van informatie en de toepasselijke beveiliging worden geregistreerd in het register van verwerkingen.

HOOFDSTUK 4 SLOTARTIKELEN

ARTIKEL 4.1 INWERKINGTREDING

1. Het Privacyprotocol ICT-middelengebruik is vastgesteld op 23 maart 2021, nummer 1069027/1586306.
2. Dit Protocol treedt in werking op 13 april 2021.

Toelichting

ARTIKELSGEWIJZE TOELICHTING

ARTIKEL 1.2 DEFINITIES

Met logging wordt bedoeld de vastlegging van gebeurtenissen in de ICT-middelen, onder andere gebeurtenissen die voortvloeien uit het gebruik ervan door wie en wanneer (en dus niet de inhoud/ het wat). Van de volgende componenten is er op het moment van vaststelling van dit protocol logging of live data beschikbaar: Netwerkcomponenten, DHCP, Direct Access, Active Directory, System Center Configuration Manager, File Servers, Email, Office 365/Azure, Printing en Anywhere 365.

Er is in de eerste plaats sprake van een incident in het geval van een (vermoeden van een) handeling die in strijd is met de afgelegde eed of belofte of met de provinciale gedragscode. Een vermoeden bestaat alleen als de verdenking onderbouwd kan worden en aangegeven kan worden waarop het vermoeden is gebaseerd (bijv. door een collega waargenomen). Bedoeld wordt dus niet dat het vermoeden bewezen moet kunnen worden vóórdat gericht gecontroleerd mag worden. Daartoe dient immers het hierna te volgen onderzoek conform artikel 2.3 en/of 2.4.

Hiernaast kan ook sprake zijn van een incident in het geval de provincie dient mee te werken aan een onderzoek waarbij bewijs verzameld wordt voor het opsporen van betrokkenen die zich aan een strafbaar feit schuldig hebben gemaakt met behulp van de ICT-middelen. Hierbij kan worden gedacht aan het meewerken op bevel van de politie.

Met de integriteitsverklaring wordt bedoeld de verklaring die externen in het kader van de integriteit ondertekenen.

Voorbeelden van incidenten zijn fraude, het lekken van vertrouwelijke informatie, verduistering van bewijsmateriaal of ander bescheiden, verspreiding strafbaar materiaal.

De ICT-middelen zijn ter beschikking gesteld ter ondersteuning van de functie-uitoefening. Dit betekent echter niet dat er een algeheel verbod op privégebruik van deze ICT-middelen is. Enig privégebruik is toegestaan onder de voorwaarden dat de binnen de provincie geldende voorschriften nageleefd dienen te worden, zo dient bijvoorbeeld het privégebruik incidenteel en kortstondig te zijn. Hiernaast geldt dat het privégebruik niet storend mag zijn voor de dagelijkse werkzaamheden.

Met formeel leidinggevende wordt bedoeld de unitmanager en/of de sectormanager.

Bij monitoring wordt ook aangegeven het incidenteel inzien van logging. Met incidenteel wordt bedoeld de situatie waarin sprake is van storing.

ARTIKEL 1.3 REIKWIJDTE

In dit artikel is aangegeven dat dit protocol betrekking heeft op het gebruik van ICT-middelen door personeelsleden. Hiernaast dienen de medewerkers die – al dan niet direct - betrokken zijn bij de verwerking van de persoonsgegevens in het kader van dit protocol, de bepalingen van dit protocol te allen tijde in acht te nemen.

ARTIKEL 1.4 DOEL

In dit artikel is het doeleinde van de verwerking aangegeven. Dit betekent dat de verwerkingen van persoonsgegevens enkel voor het in dit artikel genoemde doeleinde gebruikt mogen worden. Voor alle andere – niet in dit artikel voorkomende – gevallen is het dus niet toegestaan.

Een nadere uitwerking van het doel:

a. tegengaan van ongeoorloofd gebruik;
b. voorkomen van negatieve publiciteit of schade aan het imago van de provincie;
c. tegengaan van seksuele intimidatie, pesten, discriminatie en andere vormen van ongewenst gedrag;
d. tegengaan van (uit)lekken van vertrouwelijke of privacygevoelige informatie;
e. bewaken van systeem- en netwerkbeveiliging;
f. kosten- en capaciteitsbeheersing van ICT-faciliteiten en -middelen.

ARTIKEL 2.1 VERZAMELING PERSOONSGEGEVENS

De registratie van logging is gebaseerd op technische monitoring, kortstondig en niet op vastlegging van persoonsgegevens. In sommige situaties zijn de gegevens te herleiden naar personen. Hiervoor moet de provincie o.b.v. persoonsgegevens (personeelsnummer of device nummer) het verzoek indienen bij leverancier. De logging betreft de volgende componenten:

a. Netwerk

De logging van netwerkcomponenten wordt niet vastgelegd via een syslog server, maar op individuele plaatsen. Enkel Fujitsu netwerkbeheerders kunnen bij deze data. De routers, switches en proxy hebben geen 'vaste' logging beschikbaar.

In Wireless LAN Controller kunnen errors worden gezien en is zichtbaar welke huidige cliënts met welke IP/Machine en met welk netwerk zijn verbonden. Deze logging wordt niet opgeslagen en is enkel real-time te volgen.

De firewall logs worden doorgestuurd naar CheckPoint managementserver. Oude logs worden automatisch verwijderd als de schijf 98304 MB bereikt (hierbij geldt FIFO).

De logging van routers en switches wordt niet bewaard. Deze data is alleen real-time te volgen. Ook op de proxy wordt geen logging bewaard.

b. DHCP

Hierbinnen wordt er gelogd welke device een IP-adres verkrijgt. De audit logging van de DHCP-server wordt elke 7 dagen overschreven. Enkel Fujitsu beheerders kunnen bij de logging komen.

c. Direct Access

Op deze server wordt er gelogd welke gebruiker vanaf welke laptop een verbinding maakt. De logging bevat de verbonden cliënts. Het is mogelijk een rapport te maken van de gebruiker of machine. In dit rapport staan IP-adressen en protocollen. Er wordt geen logging gemaakt van wat de gebruikers benaderen. Alleen Fujitsu beheerders kunnen de Direct Access logging opvragen.

d. Active Directory

Hierbij worden geen specifieke logbestanden aangemaakt, alleen de standaard event logbestanden. Deze eventlogs bevatten de authenticatie en specifieke audit details van gebruikers en werkplekken. Deze logging is alleen op te vragen door Fujitsu beheerders met gedelegeerde rechten.

e. System Center Configuration Manager (SCCM)

Hierin worden de koppelingen gemaakt tussen gebruikers en werkplekken. Dit is nodig voor het uitrollen en distribueren van werkplekken en software. Alleen Fujitsu SCCM Administrators kunnen bij deze logging.

f. File Servers/Back-up

Voor de fileservers is geen logging beschikbaar, maar wel gebruikers- en afdelingsdata. Deze data wordt bewaard op een fileserver. Van de fileservers worden back-ups gemaakt. De back-upservers hebben meerdere kopieën van data welke kunnen worden 'gerestored'. Deze logging bevat geen gebruikers-of auditingdata.

g. Email

Al het email verkeer wordt gelogd op de exchange servers. Dit betreft messagetracking. In deze logging staat wie welk email-bericht heeft gestuurd, naar wie het gestuurd is en vanaf welke server het afkomstig is. Deze exchange logging gaat 30 dagen terug en wordt vervolgens overschreven. Alleen Fujitsu Exchange beheerders kunnen bij deze logging.

h. Office 365

De logging gaat hier van Message tracking tot aan rapporteren van het lebruik van Office 365, Email, OneDrive, Security, SharePoint etc. Alleen Office 365 Administrators kunnen bij deze logging en rapportages. De rapportages gaan terug tot 180 dagen.

ARTIKEL 2.2 TOEGANG TOT, INZAGE IN EN VERSTREKKING VAN LOGGING EN ANDERE PERSOONSGEGEVENS

In dit artikel is de toegang tot de vastgelegde gegevens geregeld. Aangegeven is o.a. dat inzage beperkt is tot die gevallen waarin sprake is van een (vermoeden van een) incident. Dit artikel dient in samenhang met artikel 2.3 gelezen te worden. Logging kan namelijk enkel in het kader van een onderzoek worden opgevraagd en ingezien.

Met hetgeen is vermeld in lid 7 wordt bedoeld de check (controle) die doorlopend (steekproefsgewijs) en incidenteel (dus in het geval zich een technisch probleem voordoet) door de beheerder(s) van het ICT-middel wordt gedaan (met andere woorden monitoring).

ARTIKEL 2.3 ONDERZOEK EN INLICHTING PERSONEELSLID BIJ LOGGING

In dit artikel worden de voorwaarden genoemd die in acht genomen moeten worden zowel vóórdat het onderzoek plaats kan vinden als tijdens het onderzoek.

Alvorens inzage in logging kan plaatsvinden dient onderzocht te worden of niet volstaan kan worden met minder ingrijpende middelen.

In dit artikel is ook aangegeven dat de FG om advies dient te worden gevraagd alvorens de vastgelegde gegevens worden ingezien. Het is echter te allen tijde aan de FG om te bepalen of dit ook inderdaad nodig is in het betreffende geval.

In dit artikel is met betrekking tot de verwijdering aangesloten bij een periode van 6 maanden respectievelijk 1 jaar. Hiervoor is gekozen met het oog op een eventueel geschil. Indien echter het personeelslid verzoekt om éérdere verwijdering, dient dit (indien mogelijk) gehonoreerd te worden.

Na sluiting van het onderzoek dienen alle betrokkenen bij het onderzoek alle gerelateerde correspondentie, overige gegevens en documenten te verwijderen. Hierbij kan onder andere gedacht worden aan e-mails en eigen aantekeningen waarin persoonsgegevens voorkomen in het kader van het onderzoek.

ARTIKEL 2.4 ONDERZOEK EN INLICHTING PERSONEELSLID BIJ OBSERVATIE

Aangegeven wordt wanneer een onderzoek middels observatie gerechtvaardigd is. Het dient hierbij te gaan om een redelijk vermoeden van een incident in de vorm van een misdrijf of misbruik, waarbij inzage in de inhoud van berichten/mappen etc. noodzakelijk is om de waarheid te achterhalen. Alvorens observatie kan plaatsvinden dient tevens sprake te zijn van een noodzaak hiertoe. Allereerst dient dus onderzocht te worden of niet kan worden volstaan met minder ingrijpende middelen. Het is afhankelijk van de omstandigheden van het geval, aan welke ingrijpende middelen gedacht kan worden.

In geval van een onderzoek als bedoeld in dit artikel dient het personeelslid eveneens hierover te worden geïnformeerd vóórdat observatie kan plaatsvinden, tenzij sprake is van gevreesde vrees. Hierbij kan gedacht worden aan bijvoorbeeld:

a. verandering gedragslijn dan wel verwijdering bewijsmateriaal of
b. op bevel van een daartoe bevoegde instantie dient het onderzoek heimelijk te gebeuren.

In dit artikel is met betrekking tot de verwijdering aangesloten bij een periode van 6 maanden respectievelijk 1 jaar. Hiervoor is gekozen met het oog op een eventueel geschil. Indien echter het personeelslid verzoekt om éérdere verwijdering, dient dit (indien mogelijk) gehonoreerd te worden.

Onderzoek met betrekking tot een personeelslid met een vertrouwensfunctie wordt uitgevoerd door een extern bureau. Dit om te voorkomen dat berichten verband houdende met de vertrouwensfunctie kunnen worden ingezien.

ARTIKEL 3.1 AANVULLENDE BEWAARTERMIJN BIJ OBSERVATIE

De termijn van 6 maanden respectievelijk 1 jaar, genoemd in de artikelen 2.3 en 2.4, geldt niet in het geval het onderzoek wordt heropend. In dat geval geldt artikel 3.1.

Datum datalek	Datum constatering datalek	Feiten omtrent het datalek	Betrokken externe organisaties	Gevolgen van het datalek	Genomen corrigerende maatregelen	Preventieve maatregelen	Functionaris Gegevensbescherming betrokken	Melding gedaan aan de AP?	Reden waarom wel/niet gemeld	Datum en tijdstip melding AP	Indien geen melding binnen 72 uur: reden waarom	Melding gedaan aan betrokkene(n)?	Reden waarom wel/niet gemeld	Datum en tijdstip melding betrokkene(n)	Wat is er gecommuniceerd aan betrokkene(n)	Voorlopige of definitieve melding?	Ingetrokken?
??	28-1-2025	CV's staan op open sites van SharePoint en zijn dus in te zien door iedereen binnen de provincie	geen	naw e-mailadres en telefoonnummer sollicitanten in te zien door de gehele organisatie	sites zijn op besloten gezet	berichtgeving op intranet over hoe om te gaan met CV's op SharePoint	ja	ja	gaat om naw, mailadressen en telefoonnummer van inhuur	29-1-2025 16.54 uur							
??	10-2-2025	Ingekomen brief van het ministerie is op de website geplaatst, waarbij de naam, telefoonnummer en mailadres van de behandelend ambtenaar niet is gelakt	geen	naam, telefoonnummer en mailadres van ambtenaar is openbaar gemaakt.	brief is van de webiste gehaald en nadat de gegevens gelakt zijn weer op de website geplaatst	menselijke fout	ja	ja	gaat om naam, mailadres en telefoonnummer van ambtenaar	11-2-25, 11.09 uur						ja	
??	16-3-2025	Gedragsverklaringen die moeten worden bijgevoegd bij een Europese aanbesteding staan op een openbare site op SP	geen	Namen, geboortedata en geboorteplaatsen van verschillende bestuurders zijn voor iedereen inzichtelijk, inclusief verklaring van goed gedrag	eerst controleren of de betreffende documenten geraadpleegd zijn en vervolgens laten verwijderen van openbare sites op SP	Er moet voorlichting komen over welke informatie niet op een openbare SP site mag opgeslagen worden.	ja	ja	voorlopige melding gedaan, mogelijk zijn de gedragsverklaringe niet ingezien door onbevoegden.	17-3-25, 16.21 uur						voorlopig	ja
11-7-2005	21-5-2025	Gepubliceerd Wob-verzoek bleek niet goed gelakt te zijn. Hierdoor werden de persoonsgegevens van de indiener in het zoekscherm van Google getoond	nee	NAW, emailadres en telefoonnummer waren voor idereeen in te zien.	Besluit is voorlopig van de website gehaald en het zoekresultaat van Google is verwijderd.	Er wordt nu op een andere manier gelakt	ja	ja	gaat om naw, mailadres en telefoonnummer van verzoeker die door iedereen gevonden kon worden	22-5-25, 14.48 uur		ja, telefonisch excuses gemaakt.					

Datum beveiligings incident	Datum constatering beveiligingsincident	Feiten omtrent het beveiligingsincident	Betrokken externe organisaties	Gevolgen van het beveiligingsincident	Genomen corrigerende maatregelen	Preventieve maatregelen	Functionaris Gegevensbescherming betrokken	Melding gedaan aan de AP?	Reden waarom wel/niet gemeld
6-3-2025	6-3-2025	naam van een ambtenaar staat in het onderwerp van een document op de website van de provincie	n.v.t.	gering, alleen de naam wordt in het document genoemd.	Gevraagd om de naam uit het onderwerp van het document te verwijderen	mogelijk een fout bij het overzetten naar de nieuwe website	ja	nee	gaat alleen om de naam van een college in het onderwerp van een document.
17-3-2025	17-3-2025	VOG's staan op een openbare SharePoint site	n.v.t.	VOG's mogen niet worden opgeslagen op een openbare SharePoint site. Hoewel het gaat om positieve informatie, er zijn geen belemmeringen om de betreffende personen aan te nemen, hoort deze informatie daar niet opgeslagen te worden	Gevraagd om de VOG te verwijderen van de openbare SharePoint site	menselijke fout	ja	nee	uit de audit trail blijkt niet dat onbevoegden het document hebben ingezien. Er zal wel onderzocht worden hoe we dit in de toekomst kunnen voorkomen dat dergelijke informatie op een openbare SharePoint site wordt opgeslagen.
23-4-2025	23-4-2025	TopDesk: sommige behandelaren kunnen ook bij TopDesk vragen waarvan ze geen behandelaar zijn.	n.v.t.	sommige behandelaren in TopDesk hadden ook toegang tot vragen waar ze geen behandelaar van waren; konden daardoor naw gegevens van collega's inzien.	Gevraagd om de toegang van de behandelaren te beperken	menselijke fout	ja	nee	er is niet gebleken dat behandelaren de aanvragen die niet voor hen waren hebben opgepakt.
19-9-2024	15-5-2025	Groepen die lid zijn van deze Service offerings hebben toegang tot de informatie van incidenten. Om 14:51 is er vastgesteld dat het gevolg hiervan is dat hierdoor Sogeti medewerkers in India toegang hebben gehad tot tickets waarvoor geldt dat deze een datarestrictie binnen de Europese Economische Ruimte (EER) hadden. Dit betekent dat medewerkers van de Capgemini groep in India toegang hebben gehad tot een aantal service tickets waar ze normaal gesproken geen toegang toe zouden hebben. Ze hebben ook daadwerkelijk een aantal tickets bekeken. Ik wil benadrukken dat onze corporate binding rules van toepassing blijven en dat er geen gegevens zijn ingezien door andere klanten.	Sogeti	Medwerkers in India hadden toegang tot gemelde ICT problemen. Uit de audittrail bleek dat de melding die is ingezien geen gevoelige informatie bevat.	Het lek is inmiddels gedicht.	menselijke fout	ja	nee	geen risico gelet op de inhoud van de melding die is ingezien.
23-7-2025	24-7-2025	Via SharePoint is er toegang gegeven aan derde voor bepaalde informatie. Het bleek al snel dat deze derden toegang hadden tot meer informatie binnen SP dan nodig.	n.v.t.	persoonsgegevens (namen) en documenten over andere ondewerpen waar in te zien door derden	Het lek is inmiddels gedicht.	menselijke fout	ja	nee	De link is meteen ongedaan gemaakt. De derden waren andere overheidsinstanties / semi-overheidsinstellingen. Er is gevraagd aan de derden om de link niet te gebruiken en te verwijderen.
15-9-2025	15-9-2025	naam van een ambtenaar staat in het onderwerp van een document op de website van de provincie	gemeente	gering, het gaat alleen om de naam en handtekening van een ambtenaar	Er is gevraagd om de gegevens te verwijderen	MENSELIJKE FOUT	JA	nee	gelet op de aard van de gegevens een klein risico
?	9-12-2025	Site MWO blijkt op openbaar te staan i.p.v. besloten	n.v.t.	gegevens van collega's over pensioen waren voor iedereen in te zien	De site staat nu op vertrouwelijk	menselijke fout	JA	nee	site is meteen op besloten gezet, niet gebleken dat anderen wat met deze informatie hebben gedaan.
28-1-2026	29-1-2026	mail met bijlage verzonden aan verkeerde ontvanger	n.v.t.	geen, in de bijlage stond alleen het naam van het bedrijf en gegevens van PNH	voor de zekerheid gevraagd de bijlage te deleten	menselijke fout	JA	nee	gelet op de aard van de gegevens geen risico
3-2-2026	2-2-2026	Site met documenten met persoonsgegevens blijkt openbaar te zijn, oa. BSN	n.v.t.	BSN moet niet voor iedereen in te zien zijn	document is nu afgeschermd, uit onderzoek blijkt dat het niet geraadplaagd is	menselijke fout	JA	nee	niet is gebleken dat anderen de informatie hebben geraadpleegd
23-3-2026	24-3-2026	bestand met zakellijke mailadressen verzonden naar het verkeerde adres	n.v.t.	zakelijke mailadressen waren in te zien door een bedrijf waar ze niet voor bedoeld waren	De e-mail is door het betreffende bedrijf verwijderd	menselijke fout	JA	nee	de mail is verwijderd en het ging om zakelijke e-mailadressen