Veldhoven

GEMEENTEBLAD

Officiële uitgave van de gemeente Veldhoven

Nr. 278463

24 december 2018

INFORMATIE BEVEILIGINGSBELEID GEMEENTE VELDHOVEN 2019 - 2021

Samenvatting en vaststelling

De hele organisatie heeft een belangrijke taak en verantwoordelijkheid in relatie tot informatiebeveiliging. Het is van groot belang dat de informatie die we gebruiken Beschikbaar, Integer en Vertrouwelijk blijft. Wanneer we hierin niet slagen, is de mogelijke schade aanzienlijk. De noodzaak tot informatiebeveiliging vloeit voort uit de wettelijke taken die we als gemeente uitvoeren. We streven ernaar om volgens de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG, in de toekomst Baseline Informatiebeveiliging Overheid BIO) normen te werken om een optimaal niveau van informatieveiligheid te bereiken.

Informatiebeveiliging is een continu proces. De komende jaren blijven we werken aan het verhogen van informatieveiligheid en een hogere mate van bewustzijn. Om dit te bereiken zijn een aantal speerpunten gedefinieerd. We brengen meer structuur aan in het bepalen en uitzetten van maatregelen, we gaan data classificeren en we zorgen voor verdere professionalisering en bewustwording van de gehele organisatie ten opzichte van informatieveiligheid.

De stand van informatieveiligheid wordt op diverse manieren gecontroleerd en de rapportage en verantwoording hierover vindt plaats in verschillende gremia: het Management Team, het College van B&W en de Gemeenteraad. Informatiebeveiliging wordt hierdoor onderdeel van de Planning en Control cyclus.

Met de vaststelling van dit Informatiebeveiligingsbeleid benadrukt het College het belang van informatiebeveiliging en worden de algemene uitgangspunten vastgelegd.

Inleiding

Het informatiebeveiligingsbeleid geeft algemene beleidsuitgangspunten over informatiebeveiliging. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. Dit informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving. Het is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
Naast het informatiebeveiligingsbeleid hanteren we een informatiebeveiligingsplan. In het informatiebeveiligingsplan worden de beleidsuitgangspunten nader uitgewerkt.

Het belang van informatieveiligheid

Informatiebeveiliging doen we niet zomaar. Het is van toenemend belang dat de gemeente Veldhoven haar informatie goed beschermt. We verwerken namelijk steeds meer informatie van, over en voor inwoners om haar taken en diensten uit te voeren. Inwoners en bedrijven in de gemeente moeten erop kunnen vertrouwen dat hun gegevens juist zijn. We zorgen ervoor dat gegevens niet in handen vallen van onbevoegden maar wel beschikbaar zijn wanneer dat nodig is. Verlies of manipulatie van gegevens door onbevoegden en uitval van ICT voorzieningen kunnen namelijk ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade.

We voeren verschillende wettelijke taken en diensten uit zoals de Basisregistratie personen (BRP), de Paspoort Uitvoeringsregeling Nederland (PUN), de Basisregistratie Adressen en Gebouwen (BAG), de Basisregistratie Grootschalige Topografie (BGT), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Wet maatschappelijke ondersteuning (Wmo), de Jeugdwet, de Participatiewet etc. en moeten daarom voldoen aan de opgestelde kaders. Om de (privacy)rechten van onze inwoners te waarborgen, bevatten deze wettelijke kaders regels over de omgang met gegevens. Naast gemeentelijke wetgeving, moet de gemeente ook rekening houden met Europese wetgeving en de nationale uitvoeringswetten hiervan, zoals de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene gegevensbescherming (UAvg). Wet- en regelgeving vraagt diverse inspanningen op het gebied van informatiebeveiliging en kent in sommige gevallen een auditverplichting, zoals de ENSIA zelfevaluatie.

Daarnaast hebben alle Nederlandse gemeenten, waaronder de gemeente Veldhoven, als doel gesteld om volgens de Baseline Informatiebeveiliging Nederlandse Gemeenten (hierna: BIG) te werken. Dit normenkader kent een 'pas toe of leg uit' principe en ondersteunt verschillende wettelijke verplichtingen. Het biedt tevens houvast om informatie op een gestructureerde manier te beschermen. Met ingang van 2020 wordt de BIG vervangen door de Baseline Informatiebeveiliging Overheid (BIO), een generieke baseline voor de hele overheid.

Reikwijdte

Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, USB, SD kaart, beeldscherm et cetera) en alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen, dus ook Internet of Things (IoT is een ontwikkeling van het internet, waarbij alledaagse voorwerpen zijn verbonden met het netwerk en gegevens kunnen uitwisselen). De scope van dit beleid omvat alle gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente. Maar ook het gebruik hiervan, door medewerkers en (keten)partners in de meest brede zin van het woord en ongeacht locatie, tijdstip en gebruikte apparatuur.
Dit beleid vormt de algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen. Voorbeelden zijn BRP, PUN, BAG, BGT en Suwinet.

Doelstellingen

De afgelopen jaren hebben we hard gewerkt om de organisatie weerbaar te maken. De implementatie van verschillende technische, organisatorische en menselijke maatregelen heeft ervoor gezorgd dat er een degelijke basis is gelegd. We streven ernaar om 'in control' te zijn op het gebied van informatiebeveiliging en daarover op professionele wijze verantwoording af te leggen. In control betekent dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn. Dit geheel wordt verankerd in de Planning en Control cyclus.

Doelstellingen:
Dit informatiebeveiligingsbeleid (IB-beleid) is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente Veldhoven voldoet aan relevante wet en regelgeving. Gemeente Veldhoven streeft er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen. In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus. De komende jaren blijven we werken aan het verhogen van informatieveiligheid en een hogere mate van bewustzijn.

Om dit te bereiken brengen we meer structuur aan in het bepalen en uitzetten van maatregelen en borgen we dat in de P&C cyclus. We gaan data classificeren om te voldoen aan de eisen van de BIG op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid en zo te bepalen hoe er met de desbetreffende gegevens moet worden omgegaan, welke maatregelen daarvoor nodig zijn en hoe deze gegevens te benaderen zijn en door wie.

Het grootste risico in informatiebeveiliging blijft de mens. Daarom streven we naar een verdere professionalisering en een hoger bewustzijn binnen alle lagen van de organisatie. Het is van groot belang dat iedereen die met vertrouwelijke gegevens werkt, zich bewust is van de mogelijke risico's en daarnaar handelt. Nieuwe en bestaande processen en systemen worden vormgegeven met informatiebeveiliging als vereiste.

Uitvoering

Risicomanagement en maatregelenstructuur

Informatiebeveiliging vereist het treffen van maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen de organisatie te waarborgen. Informatiebeveiliging moet ervoor zorgen dat eventuele gevolgen van incidenten tot een acceptabel niveau beperkt zijn. Om de beschikbare middelen zo effectief en efficiënt mogelijk te benutten, wordt risico gebaseerd gewerkt. Het uitgangspunt is dat prioriteit wordt gegeven aan de grootste dreigingen op het gebied van (vertrouwelijke) informatie en de continuïteit van dienstverlening. In geval van

beveiligingsincidenten, worden de 'Operationele procedure omgaan met informatiebeveiligingsincidenten gemeente Veldhoven 2016' en (indien nodig) de procedure datalekken gehanteerd.

De risico's zijn (in lijn met de BIG) centraal in kaart gebracht, vastgelegd en beoordeeld. Dit is een taak van de informatiebeveiligingsorganisatie. Vastlegging vindt plaats in een Information Security Management Systeem (ISMS). Dit systeem maakt risico's, BIG normen en verschillende documenten inzichtelijk. Tevens kunnen hiermee acties worden uitgezet naar verschillende personen en organisatieonderdelen. Om risico's centraal te kunnen beheersen, heeft de gemeente risicomanagement en interne controle op een onafhankelijke positie in de organisatie belegd.

Werkwijze:
We zetten in op een gestructureerde aanpak om risico gebaseerd te kunnen werken. Dit vereist een adequaat gebruik van het ISMS en heldere afspraken over verantwoordelijkheden tussen de informatiebeveiligingsorganisatie, management en gebruikers.

De informatiebeveiligingsorganisatie adviseert het MT over de risico's. Het bepalen van vervolgacties is een verantwoordelijkheid van het MT en het college van B&W. Afdelingshoofden bepalen welke maatregelen noodzakelijk zijn om het risico te beperken of te verhelpen en wie dit uit gaat voeren. Ook kunnen zij ervoor kiezen om risico's te accepteren. De door hen gekozen acties worden vastgelegd in het ISMS. Het college van B&W wordt minimaal eens per jaar over de status van de informatiebeveiliging en de grootste risico's geïnformeerd.

Jaarlijks zal een uitvoeringsplan worden opgesteld met daarin de activiteiten op het gebied van informatiebeveiliging en privacy.

Verwerking van (persoons)gegevens en toegangsbeveiliging

Om de veiligheid van verwerking van vertrouwelijke gegevens te kunnen garanderen, worden er eisen gesteld aan gemeenten. Er moeten organisatorische maatregelen worden genomen op het gebied van wijzigingsbeheer, functiescheiding, patchmanagement en incidentmanagement.

We verzamelen gegevens over inwoners voor (vooraf) bepaalde doelen. Deze gegevens worden door medewerkers opgeslagen in verschillende applicaties en basisregistraties om ze te kunnen gebruiken voor deze doeleinden. Bij een dergelijke verwerking worden alleen die data verwerkt, die noodzakelijk zijn voor een goede afhandeling van het proces of de procedure. De uitgangspunten voor omgang met vertrouwelijke gegevens zijn te vinden in de Algemene Verordening Gegevensbescherming en nader geconcretiseerd in het privacy beleid en - reglement van de gemeente Veldhoven.

Dataclassificatie
We gaan data classificeren om te voldoen aan de eisen van de BIG op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid.

In veel gevallen gaat het bij dataclassificatie om persoonsgegevens. Ook interne gegevens over onze bedrijfsvoering kennen een vertrouwelijkheidsgraad.

Alle gegevens die de gemeente verwerkt voor het uitvoeren van haar taken worden onderverdeeld in verschillende gradaties van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Dit heet dataclassificatie. Deze gradaties bepalen welke maatregelen moeten worden getroffen voor de omgang met de desbetreffende gegevens en hoe deze gegevens te benaderen zijn.

Zo wordt bepaald welke authenticatiemethoden (gebruikersnaam – wachtwoord, pincodes e.d.) gebruikt moeten worden. Ook kunnen er extra authenticatiemiddelen nodig zijn, zoals een telefoonnummer, biometrische gegevens of bijvoorbeeld een badge, pas of token. De Beschikbaarheid bepaalt de mate waarin gegevens toegankelijk moeten zijn; sommige informatie moet bijvoorbeeld altijd beschikbaar zijn omdat processen hiervan direct afhankelijk zijn. Integriteit geeft aan in hoeverre de informatie juist, volledig en actueel moet zijn. Vertrouwelijkheid bepaalt wie toegang heeft tot de informatie. De klassen van vertrouwelijkheid zijn: openbaar, bedrijfsvertrouwelijk (interne gegevens), vertrouwelijk (persoonsgegevens van inwoners) en geheim (bijvoorbeeld strafrechtelijke of medische gegevens). De manier waarop we omgaan met dataclassificatie wordt verder uitgeschreven in dataclassificatieregels.

Fysieke toegangsbeveiliging
Toegang tot de gegevens die de gemeente verwerkt, is beperkt. Fysieke toegang tot gegevens is beperkt door het aanbrengen van zones op gemeentelijke locaties en gebouwen. Alleen medewerkers met de

juiste autorisaties kunnen toegang krijgen tot beveiligde zones. In deze zones zijn werkplekken te vinden en er staan afsluitbare opbergruimtes voor dossiers.

Naast de beveiligde zones, zijn er zones ingericht waar toegang nog beperkter is, zoals kluis- en serverruimtes. Er zijn extra maatregelen getroffen om personeel te beschermen tegen (fysieke) bedreiging, geweld, manipulatie en andere dreigingen. Voorbeelden hiervan zijn opleidingen en trainingen. Om alles in goede banen te leiden, is de verantwoordelijkheid voor fysieke toegang belegd bij het afdelingshoofd Facilitair bedrijf, die rekening houdt met de eisen en wensen vanuit het perspectief van informatieveiligheid. De toegang tot het gebouw wordt geregistreerd met beveiligingscamera's.

Digitale toegangsbeveiliging
Via de digitale werkplekken kunnen medewerkers toegang krijgen tot interne systemen en informatie. Er zijn bedrijfsmiddelen uitgereikt waarmee ook buiten de werkplekken toegang tot systemen mogelijk is. In deze gevallen is het 'Protocol veilig en integer werken met informatie en informatietechnologie' van toepassing.

Toegang tot applicaties en systemen waarin vertrouwelijke gegevens worden verwerkt, is ook beperkt. Er is autorisatiebeheer ingericht, waardoor toegang tot deze gegevens alleen mogelijk is voor medewerkers die daar recht op hebben. Om deze toegang goed te kunnen regelen, heeft de gemeente toegangsrichtlijnen en -protocollen opgesteld, waaronder de in-/uitdienstprocedure en mutaties. Daarin wordt door het verantwoordelijke afdelingshoofd bepaald wanneer, in welke gevallen en aan wie toegang wordt verleend. Dit geldt zowel voor vaste medewerkers, als voor ingehuurde medewerkers. Leveranciers hebben beperkt toegang, waarbij per geval goedkeuring vereist is en in alle gevallen registratie van toegang plaats vindt.

Jaarlijks vindt evaluatie plaats van de rechten die uitgegeven zijn. Dit vindt zowel fysiek als logisch plaats. Hierbij worden extra rechten, waaronder toegang tot extra gevoelige ruimtes en toegang tot bepaalde kritische applicaties, halfjaarlijks gecontroleerd. Deze en andere controles worden vastgelegd en expliciet afgetekend door de verantwoordelijke.

Voor uitwisseling en opslag van informatie maakt de gemeente gebruik van gegevensversleuteling of andere passende beveiligingsmaatregelen. Op deze manier is de verwerking van informatie door of namens de gemeente gewaarborgd.

Organisatie

Organisatiebeveiliging is een gemeenschappelijke verantwoordelijkheid van alle medewerkers. Iedereen dient zich te houden aan de gedragscode die hiervoor gelden, zoals geheimhouding en privacyrichtlijnen. Daarnaast heeft elke medewerker van de gemeente een Verklaring Omtrent Gedrag overlegd (voor bestaande medewerkers gebeurt dit in fasen) en een ambtseed afgelegd. Voor het gebruik van de middelen van de gemeente – zowel telefoons, als laptops en andere fysieke middelen, maar ook gegevens voor de uitvoering van het werk – tekent de medewerker een bruikleenovereenkomst, waarin de medewerker op de hoogte wordt gesteld van de kaders die hiervoor gelden. Deze kaders worden beschikbaar gesteld op Vicky en medewerkers worden geïnformeerd wanneer er wijzigingen zijn.

Bijzondere taken en verantwoordelijkheden
Een aantal personen en organisatieonderdelen heeft een bijzondere taak of verantwoordelijkheid als het gaat om informatiebeveiliging. Het College van B&W draagt de eindverantwoordelijkheid op het gebied van informatiebeveiliging. Het College wordt geïnformeerd door de informatiebeveiligingsorganisatie en bespreekt de risico's met het management. Ook legt het College verantwoording af aan de Raad, die een toezichthoudende functie heeft.

Het management heeft een dubbele rol in informatiebeveiliging. Afdelingshoofden hebben een verantwoordelijkheid in risicomanagement, maar sturen ook op informatieveiligheid en het verhogen van bewustzijn in hun afdeling.

De gemeente Veldhoven draagt er zorg voor dat de medewerkers met een rol in de organisatie van informatieveiligheid voldoende getraind zijn en blijven op het gebied van informatiebeveiliging en privacy.

Informatiebeveiligingsorganisatie
Om het beleid vorm te geven en te borgen, heeft de gemeente een aantal specifieke taken en verantwoordelijkheden belegd bij de informatiebeveiligingsorganisatie. De informatiebeveiligingsorganisatie bestaat uit de Informatiebeveiligingsfunctionaris (IBF), de coördinator

DIV, de Functionaris Gegevensbescherming (FG), de coördinator I/A, de concerncontroller en de privacy officer. Samen vormen zij het team Informatiebeveiliging en Privacy (IB&P). Team IB&P voert structureel overleg om de status van informatiebeveiliging en privacy in de organisatie te bespreken.

De invoering van maatregelen wordt gecoördineerd en gecontroleerd door de IBF. Dit gebeurt na een zorgvuldige risicoafweging, waarbij risico's worden geprioriteerd en maatregelen worden vastgesteld, uitgevoerd en geëvalueerd. De IBF rapporteert over de risico's en de maatregelen aan het managementteam en aan het College van B&W.
De IBF geeft binnen de organisatie gevraagd en ongevraagd advies over informatiebeveiliging. De IBF treedt daarnaast op als ENSIA coördinator (met ENSIA vinden verschillende audits binnen verschillende domeinen plaats).

De FG ziet erop toe dat de gemeente de privacywetgeving naleeft en inwoners hun recht op privacy kunnen uitoefenen ten opzichte van de gemeente. De FG is onafhankelijk en adviseert over de uitleg van de verplichtingen uit de privacywetgeving. In geval van tekortkomingen rapporteert de FG aan het College van B&W. De FG is ook het aanspreekpunt van de gemeente, wanneer de Autoriteit Persoonsgegevens (de privacy toezichthouder van Nederland) vragen heeft over de manier waarop de gemeente uitvoering geeft aan de privacywetgeving. De FG houdt toezicht op de naleving van privacywetgeving, maar voert niet uit.

De privacy officer (PO of ook wel juridisch adviseur privacy) is verantwoordelijk voor het vormgeven en bewaken van het privacy beleid binnen de gemeente. Daarnaast ondersteunt de PO bij het in kaart brengen van de risico's door bijvoorbeeld een Data Privacy Impact Assessment (DPIA) uit te laten voeren. De PO speelt ook een belangrijke rol op de werkvloeren en heeft net als de IBF een adviserende rol richting vak afdelingen.

Tijdens ernstige beveiligingsincidenten of datalekken, komt het Cyber Incident Response Team (CIRT) bijeen. Het CIRT bestaat uit het IB&P team, aangevuld met medewerkers van verschillende afdelingen (Communicatie, Juridische Zaken, P&O, Financiën, Automatisering, Management, bestuur). Het CIRT bepaalt de vervolgacties om incidenten op te lossen en om de nadelige gevolgen zo veel mogelijk te beperken. Ook eventuele externe communicatie over incidenten wordt voorbereid in het CIRT. Om in geval van incidenten snel en adequaat te kunnen handelen, vinden periodieke oefeningen plaats.

Samenwerking

Team IB&P neemt deel aan verschillende projecten en aanbestedingen om ervoor te zorgen dat Informatiebeveiliging en Privacy op de juiste manier wordt ingebed in de bedrijfsvoering. Er vindt afstemming plaats met verschillende bedrijfsonderdelen om planningen op elkaar af te stemmen.

De informatiebeveiligingsorganisatie overlegt periodiek met de informatiebeveiligingsorganisatie in Best en neemt deel aan diverse externe overlegstructuren en kennisgroepen, zoals de VNG met in het bijzonder de Informatiebeveiligingsdienst (IBD) en aan verschillende regionale overleggen.
Ook werken de IBF en de privacy officer nauw samen met dezelfde functionarissen uit Best.
Daarnaast zoekt team IB&P aansluiting bij landelijke initiatieven en ontwikkelingen, zoals Digitale Agenda 2020 en Gemeentelijke Gemeenschappelijke Infrastructuur (GGI).

Bewustwording (awareness)
De mens is de zwakste schakel in de informatiebeveiliging. Om als organisatie adequaat te kunnen reageren op cyberdreigingen, beveiligingsincidenten en datalekken is het daarom van groot belang om medewerkers zo goed mogelijk voor te bereiden. Medewerkers dienen op de hoogte te zijn van de extra risico's die werken met vertrouwelijke gegevens met zich mee brengen, maar ook van organisatie brede procedures om incidenten en datalekken te melden.

De gemeente Veldhoven zorgt ervoor dat medewerkers risico's en hun verantwoordelijkheden kennen. Medewerkers gaan op een juiste manier met (vertrouwelijke) informatie om, herkennen verschillende dreigingen en weten hoe ze hiermee om moeten gaan.

Om dit te bereiken, voert de informatiebeveiligingsorganisatie jaarlijks en cyclisch activiteiten uit om bewustwording bij medewerkers te vergroten, gesteund door het management en het College van B&W.

Binnen de organisatie zijn verschillende technische maatregelen en tools geïmplementeerd die medewerkers faciliteren om hun werk veilig uit te voeren. Het is belangrijk dat medewerkers weten in

welke situaties deze gebruikt moeten worden en hoe hiernaar te handelen. Op deze manier borgen we dat de organisatie weerbaar is tegen (cyber)aanvallen en dat (vertrouwelijke) informatie altijd zo adequaat als mogelijk beschermd wordt. Medewerkers worden met nieuwsberichten op Vicky op de hoogte gehouden van de ontwikkelingen op het gebied van informatiebeveiliging. Hier worden ook beleidsstukken, protocollen en aanvullende informatie beschikbaar gesteld.

Communicatie
We voeren open communicatie via diverse kanalen (website, discussieplatforms, etc.) over de manier waarop informatieveiligheid en privacy geborgd is en onderdeel uitmaakt van de cultuur van onze organisatie. Op de website van gemeente Veldhoven zijn diverse documenten te vinden over de manier waarop we met informatie en privacy omgaan en welke richtlijnen en beleidstukken daarvoor worden gehanteerd. Ook is daar terug te vinden bij wie betrokkenen met klachten of vragen terecht kunnen en hoe ze een klacht of vraag kunnen indienen.

Controle
Toetsing aan en naleving van wet- en regelgeving
Om te zorgen dat de gemeente blijft voldoen aan geldende wet- en regelgeving worden de organisatie en de werkwijze regelmatig getoetst. Dit gebeurt door audits, zoals de jaarrekeningcontrole en andere audits door de accountant en externe auditors enerzijds en door interne auditors anderzijds. Om deze toetsen goed te kunnen doorstaan, dient een bepaald minimaal niveau aan informatiebeveiliging behaald te worden. Medewerkers die hierin een verantwoordelijkheid hebben, bespreken de status van informatieveiligheid en plannen en nemen noodzakelijke stappen om de bescherming van gevoelige gegevens daar waar nodig aan te scherpen.
Jaarlijks vinden zelfevaluaties plaats en legt de organisatie verantwoording af aan het College van B&W met de ENSIA systematiek. In de ENSIA cyclus vindt ook een verplichte audit plaats voor de DigiD aansluitingen en Suwinet. Deze audit wordt uitgevoerd door een onafhankelijke auditor en wordt voorbereid door medewerkers van de organisatie en de ENSIA-coördinator.

Naast de audits in het kader van ENSIA, vinden binnen de organisatie nog verschillende andere controles en audits plaats, zoals een IT audit op financiële systemen en processen, een audit op werkprocessen en verbijzonderde interne controles. Deze audits en controles zijn verder omschreven in het Interne controleplan gemeente Veldhoven.

Logging
Het is belangrijk om te kunnen achterhalen welke gebeurtenissen hebben geleid tot incidenten. Om dit te kunnen doen, is er logging ingericht op kritische systemen en applicaties. We voeren (interne) controle uit door de beveiliging, software en de IT omgeving regelmatig te testen in het algemeen en specifiek op zwakheden. De resultaten worden gerapporteerd aan het management, waarna dit wordt meegenomen in de Planning en Control cyclus, en in voorkomende gevallen wordt gerapporteerd aan het College van B&W.