De Haagse Scholen

BIJLAGE 8

Demarcatie service- en servicedesk per lijn domein

Datum: 11 december 2025

Versie: 1.0

1. SPOC (Single Point of Contact)

De SPoC is het eerste contactpunt voor gebruikers die IT-ondersteuning nodig hebben. De SPoC is verantwoordelijk voor de informatievoorziening aan externe IT-leveranciers of tweede-/derdelijns support voor het oplossen van incidenten, verzoeken en vragen die de SPoC zelf niet kan afhandelen. De beoordeling van de urgentie (triage) is integraal onderdeel van de werkzaamheden van de SPoC.

Taken:

- Incidentbeheer: Aannemen en registreren van alle binnenkomende incidenten / vragen /changes in de ITSM omgeving van de opdrachtnemer en vult de melding aan met de informatie die de SPoC terug krijgt van de externe partners.
- Verzoekbeheer: Aannemen van alle verzoeken in de eigen ITSM omgeving.
- Gebruikersondersteuning: Het assisteren van gebruikers bij eenvoudige vragen over hardware, Microsoft Office 365 en applicaties.
- Monitoring: Het aanspreken van de eigen IT-beheer team op openstaande tickets in de eigen ITSM omgeving conform SLA.
- Rapporteren: Het maken van rapportages van alle meldingen in de eigen ITSM omgeving volgens afspraken in de PvE.

2. IT beheer lijnen beschrijving algemeen:

1e-lijns Beheer (helpdesk)

De 1e-lijns beheer is verantwoordelijk voor het oplossen van eenvoudige incidenten en stuurt complexere zaken door naar de 2e-lijns beheer.

Taken:

- Incidentbeheer: Oplossen van binnenkomende incidenten / vragen / changes. Voert ook de eerste onderzoek uit voordat de meldingen worden doorgezet naar externe IT-leveranciers (NaaS, DVI, enz) en vult hiervoor waar nodig ook de informatie aan. Als voorbeeld: Laptop heeft geen Internetverbinding. Werkt de wifi-adapter of werkt de WLAN omgeving niet en kunnen meerdere devices niet op de WLAN.
- Verzoekbeheer: Verwerken van standaard serviceverzoeken, zoals wachtwoordresets.
- Gebruikersondersteuning: Assisteren van gebruikers met vragen over o.a. applicaties en Hardware, inclusief onderwijs-specifieke zaken of door DHS goedgekeurde hardware zoals Robots, VR-brillen en andere IoT-apparatuur.
- Monitoring: In de gaten houden van de systemen en alarmsignalen rapporteren aan de 2e lijn beheer en support-lijn.

2e-lijns Beheer (Technisch beheer)
Gespecialiseerd technisch team dat zich bezighoudt met complexere incidenten en problemen die niet door de 1e lijn opgelost kunnen worden.

Taken:

- Probleemanalyse: Diagnosticeren van de oorzaak van incidenten en identificeren van de onderliggende problemen.
- Configuratiebeheer: Maken van kleine aanpassingen in configuraties van systemen en applicaties (indien van toepassing) die niet door een CAP behandeld hoeven te worden.
- Systeemonderhoud: Uitvoeren van regulier onderhoud en updates conform het DHS-patchbeleid.
- Change management: Implementeren van veranderingen en nieuwe releases conform bijgevoegd DHS Change managementproces.

3e-lijns Beheer (experts consultant of leverancier)
De meest technisch geavanceerde supportniveau, vaak verantwoordelijk voor onderzoek en oplossing van de meest complexe problemen en voor ontwikkeling en verbetering van de IT-infrastructuur.

Taken:

- Expertanalyse: Uitvoeren van diepgaande technische analyses.

3. IT Omgeving

3.1 Local Area Network (LAN)

1e-lijns LAN-beheer
De NaaS beheerder is verantwoordelijk voor de werking van de netwerkswitches, lokale firewall en Access points.

Verantwoordelijkheid
De eerstelijns LAN-beheer is verantwoordelijk voor de LAN verbinding tot aan de netwerkswitch van de NaaS beheerder. Doet een eerste onderzoek om uit te sluiten of het probleem niet device gerelateerd is. Als voorbeeld defect Netwerk adapter, driver of defect patch kabel. Verzamelt indien nodig informatie om de melding te kunnen doorzetten naar de NaaS beheerder.

Taken:

- Eerste beoordeling: Identificeren of een probleem device gerelateerd is (zoals een kabel die niet aangesloten of stuk is en of er meerdere devices problemen hebben met hun vaste

netwerkverbinding) of dat het moet worden doorgezet naar de NaaS beheerder.

- Communicatie: Voorziet de melding van alle informatie die de NaaS beheerder nodig heeft om de melding over te nemen. Zodat de SPoC dit kan overdragen en de gebruiker kan informeren.

3.1. Wifi/WLAN

1e-lijns Wifi-beheer
De NaaS beheerder is verantwoordelijk voor de werking van de netwerkswitches, lokale firewall en Access points.

Verantwoordelijkheid
Doet een eerste onderzoek om uit te sluiten of het probleem niet device gerelateerd is.
Als voorbeeld defect wifi-adapter. Verzamelt indien nodig informatie om de melding te kunnen doorzetten naar de NaaS beheerder.

Taken:

- Probleemidentificatie: Basisdiagnose van Wifi-gerelateerde problemen, zoals het controleren van de signaalsterkte en de beschikbaarheid van het netwerk.
- Gebruikersondersteuning: Assisteren van gebruikers bij het oplossen van eenvoudige Wifi-problemen, bijvoorbeeld door het uit- en aanzetten van Wifi op apparaten of het controleren van de netwerkinstellingen.
- Escalatie: Voorziet de melding van extra informatie voor de NaaS beheerder zodat de SPoC dit kan doorzetten.

3.2. Internet

1e-lijns Internet-beheer
Er zijn drie partijen in de keten voor het leveren van de Internet verbinding binnen een school:

- NaaS beheerder: Verantwoordelijk voor de werking van de netwerkswitches, lokale firewall en Access points.
- GlasLokaal: Verantwoordelijk voor de WAN-verbinding en de Internet feed.
- Dienst Veilig Internet: Verantwoordelijk voor de web-filters (contentfilter) en poortfiltering via de centrale firewall in de NDC. Aanpassingen zullen voorgelegd moeten worden met de ICT-afdeling van DHS.

Verantwoordelijkheid
Doet een eerste onderzoek om uit te sluiten of het probleem niet device of (W)LAN gerelateerd is en of meerdere gebruikers hier last van hebben. Verzamelt indien nodig informatie zodat de SPoC het naar de juiste partij kan doorzetten.

Taken:

- Eerste probleemdiagnose: Basisdiagnose van internetproblemen, zoals het controleren van verbindingen en het herstarten van netwerkdevices in overleg met de NaaS beheer. Onderzoeken waarom een website niet bereikbaar is, komt dit door een de web content filter van Dienst Veilig Internet of houdt Windows het tegen. Hebben meerdere scholen geen Internet door een WAN storing op de glasring van GlasLokaal.
- Gebruikersondersteuning: Hulp bieden bij eenvoudige internetproblemen, zoals het controleren van netwerkinstellingen en het oplossen van connectiviteitsissues of webbrowser instellingen.
- Escalatie: Voorziet de melding van extra informatie voor de NaaS beheerder, GlasLokaal of Dienst Veilig Internet zodat de SPoC dit kan doorzetten.

3.3. Firewalling

1e-lijns firewalling-beheer

DHS maakt gebruik van Dienst Veilig Internet, omdat de Internet feed door GlasLokaal wordt aangeboden zijn er afspraken gemaakt over de verantwoordelijkheden. GlasLokaal is volledig verantwoordelijk voor de Internet feed. Dienst Veilig Internet is verantwoordelijk voor de in stellingen van de Web content en Poort filtering. Changes aan de Web Content en Poort filtering kunnen na een CAB worden doorgevoerd. Instellingen aan de firewall op het device (bijvoorbeeld firewall van een virusscanner of Windows eigen oplossing) zal door de dienstverlener moeten worden opgepakt.

Verantwoordelijkheid
Doet een eerste onderzoek om uit te sluiten of het probleem niet device of (W)LAN gerelateerd is, een instelling op het device en of meerdere gebruikers hier last van hebben. Verzamelt indien nodig informatie om de melding te kunnen doorzetten naar de eigen IT-beheergroep, de NaaS beheerder of DHS voor het aanpassen van de firewall instellingen van Dienstveilig Internet.

Taken:

- Eerste probleemdiagnose: Basisdiagnose uitvoeren bij eenvoudige problemen zoals toegangsproblemen gerelateerd aan Windows firewall-instellingen, of een instelling in Microsoft Defender.
- Escalatie: Voorziet de melding van extra informatie voor de NaaS beheerder of de ICT-afdeling van DHS zodat de SPoC dit kan doorzetten.

3.4. Telefonie

1e-lijns Telefonie-beheer
DHS maakt gebruik van een VoIP dienst. Scholen kunnen gebruik maken van vaste en draadloze (loop) toestellen of via een mobiele Teams app. De draadloze toestellen kunnen gebruik maken van wifi of DECT. DHS heeft voorkeur voor DECT of de mobiele teams app.

Verantwoordelijkheid
Doet eerste onderzoek van het probleem, heeft de toestel een verbinding, maakt het gebruik van wifi of DECT of de Teams app. Helpen bij eenvoudige telefonie vragen.

Taken:

- Eerste probleemdiagnose: Basisdiagnose voor eenvoudige problemen zoals connectiviteitsissues of kwaliteitsproblemen (zoals ruis).
- Gebruikersondersteuning: Assisteren bij basisvragen over het gebruik van vaste telefoons en Teams Calling functies.
- Escalatie: Voorziet de melding van extra informatie zodat de SPoC dit kan doorzetten.

3.5. Azure

1e-lijns Azure beheer
De 1e-lijn biedt basisgebruikersondersteuning voor Azure-gerelateerde vragen en eenvoudige incidenten. Het doel is om de eerste problemen snel op te lossen of indien nodig door te sturen naar de 2e-lijn.

Taken:

- Eerste diagnose: Het stellen van een basisdiagnose bij meldingen van gebruikers over Azure resources om te bepalen of het probleem door de 1e-lijn kan worden opgelost.
- Basisbewaking: Eenvoudige monitoring van Azure-diensten zoals virtuele machines (VM's), cloudopslag en netwerkconnectiviteit.
- Gebruikersondersteuning: Ondersteuning bieden bij eenvoudige problemen zoals inlogproblemen of het gebruik van cloudopslag.
- Standaardvragen afhandelen: Beantwoorden van algemene vragen over het gebruik van Azure-services.
- Escalatie naar 2e-lijn: Problemen die verder gaan dan de basis, doorsturen naar de 2e- lijn.

2e-lijns Azure beheer

Verantwoordelijkheid
Ondergebracht bij de dienstverlener in combinatie met de ICT-afdeling van DHS. De 2e-lijn biedt geavanceerde technische ondersteuning voor complexere incidenten en voert meer gedetailleerde configuratie- en monitoringtaken uit binnen de Azure-omgeving.

Taken:

- Probleemoplossing: Oplossen van complexere problemen zoals het herstellen van falende VM's, het oplossen van netwerkproblemen binnen Azure, of fouten in cloudopslag.
- Configuratiebeheer: Configureren en onderhouden van Azure-resources zoals netwerken, virtuele machines en storage accounts.
- Security beheer: Toepassen van beveiligingsmaatregelen zoals het aanpassen van IAM-rollen, firewalls en beleidsregels binnen Azure.
- Performance monitoring: Monitoren van de prestaties van Azure-diensten en indien nodig optimalisaties uitvoeren.
- Escalatie naar 3e-lijn: Problemen die de expertise van de 2e-lijn overschrijden, escaleren naar de 3e-lijn voor gespecialiseerde ondersteuning.

3e-lijns Azure beheer

Verantwoordelijkheid
Microsoft in samenspraak met dienstverlener en de ICT-afdeling van DHS. De 3e-lijn biedt specialistische ondersteuning en is verantwoordelijk voor strategisch beheer van de Azure-infrastructuur. Dit omvat diepgaande analyses, architectuurontwerp en langetermijnplanning.

Taken:

- Diepgaande probleemoplossing: Oplossen van zeer complexe en kritieke incidenten zoals beveiligingsproblemen of grootschalige storingen binnen de Azure-omgeving.
- Azure-architectuurontwerp: Ontwerpen van nieuwe Azure-omgevingen of het aanpassen van bestaande infrastructuren om schaalbaarheid en veerkracht te waarborgen.
- Strategisch beheer: Evalueren en optimaliseren van resourcegebruik en kostenbeheer in Azure.
- Integratie van Azure-diensten: Integreren van Azure met andere IT-systemen, inclusief hybride cloudoplossingen.
- Beveiligingsbeheer op hoog niveau: Implementeren van Zero Trust-architecturen en compliance-gerelateerde beveiligingsmaatregelen.
- Innovatie en optimalisatie: Voortdurende verbetering van de Azure-omgeving door het implementeren van nieuwe technologieën en best practices.

3.6. Werkplekbeheer

1e-lijns Werkplekbeheer (Device Management met o.a. MS Intune)

Verantwoordelijkheid
Basisgebruikersondersteuning voor apparaten die via MDM zijn uitgerold.

Taken:

- Basisprobleemoplossing: Basisdiagnose voor eenvoudige problemen met MDM-apparaten, zonder directe aanpassingen.
- Gebruikershandleidingen: Verstrekken van handleidingen en instructies voor het gebruik van MDM-apparaten.
- Apparaat registratie: Assisteren bij het initiële registratieproces van apparaten in MDM.
- Escalatie: Voorziet de melding van extra informatie zodat de SPoC dit kan escaleren naar de 2e lijn van de IT Beheergroep om complexere problemen of kleine aanpassingen in de configuratie door te voeren.

2e-lijns Werkplek Beheer

Verantwoordelijkheid
Geavanceerde technische ondersteuning voor MDM-apparaten.

Taken:

- Geavanceerde probleemdiagnose: Diepgaande analyse en oplossing voor complexere apparaat problemen binnen MDM.
- Apparaat configuratie en -beheer: Beheren van configuraties, updates, en patches voor MDM-apparaten.
- Software-installatie: Installeren en configureren van applicaties binnen het MDM- beleid.
- Netwerkbeheer: Beheren van netwerkinstellingen en -connectiviteit specifiek voor MDM-apparaten.
- Documentatie en rapportage: Bijhouden van gedetailleerde documentatie over MDM-apparaat configuraties en probleemoplossing.
- Escalatie: Voorziet de melding van extra informatie zodat de SPoC dit kan escaleren naar de 3e lijn van de IT Beheergroep.

3e-lijns Werkplekbeheer

Verantwoordelijkheid
Specialistische en strategische ondersteuning voor complexe vraagstukken en beleidsontwikkeling voor MDM-apparaten.

Taken:

- Complexe probleemoplossing: Oplossen van technisch complexe en strategische vraagstukken binnen het MDM-framework en dit vastleggen.
- Beleidsontwikkeling en -implementatie: Ontwikkelen en implementeren van MDM- beleid en -procedures, indien DHS deze behoefte naar Opdrachtnemer uit (op afroep).
- Apparaat strategie en levenscyclusbeheer: Ontwikkelen van langetermijnstrategieën voor apparaat beheer binnen MDM, op afroep van DHS.
- Beveiligingsbeheer: Versterken en beheren van de beveiliging van MDM-apparaten conform beleid DHS.
- Leveranciers- en technologiemanagement: Evalueren en beheren van leveranciersrelaties en technologische ontwikkelingen in het MDM-domein.
- Voorbereiding CAB: Voorbereiden CAP voor het kunnen doorvoeren van complexere changes.

3.7. Microsoft 365 beheer

1e-lijns Microsoft 365 Beheer

Verantwoordelijkheid
Basisgebruikersondersteuning en probleemoplossing voor Microsoft 365- toepassingen.

Taken:

- Gebruikersvragen: Assisteren van de SPoC bij basisvragen over Microsoft 365- applicaties van gebruikers.
- Basisprobleemoplossing: Eenvoudige problemen oplossen zoals loginproblemen, basisfuncties van apps zoals Outlook, Word, Excel, etc.
- Documentatie: Verstrekken van gebruikershandleidingen en instructies voor standaard Microsoft 365-functies aan de ICT-afdeling van DHS zodat zij dit kunnen publiceren
- Accountbeheer: Helpen bij het resetten van het wachtwoord.
- Escalatie: Voorziet de melding van extra informatie zodat de SPoC dit kan escaleren naar de 2e lijn van de IT Beheergroep.

2e-lijns Microsoft 365 Beheer

Verantwoordelijkheid
Geavanceerde technische ondersteuning en beheer van Microsoft 365- applicaties en -diensten.

Taken:

- Geavanceerde probleemdiagnose: Oplossen van complexere problemen met Microsoft 365-apps en -diensten.
- Beheer van gebruikersrechten: Beheren en configureren van afgesproken gebruikersrechten en toegang binnen de Microsoft 365-omgeving.
- Beheer van applicatie-instellingen: Configureren en beheren van kleine instellingen voor specifieke Microsoft 365-applicaties.
- Beveiligingsbeheer: Monitoren en beheren van beveiligingsinstellingen en -beleid binnen Microsoft 365.
- Documentatie en rapportage: Bijhouden van gedetailleerde documentatie over configuraties en opgeloste problemen.
- Escalatie: Voorziet de melding van extra informatie zodat de SPoC dit kan escaleren naar de 3e lijn van de IT Beheergroep.

3e-lijns Microsoft 365 Beheer

Verantwoordelijkheid
Expertise in complexe integraties, beleidsontwikkeling en strategisch beheer van Microsoft 365.

Taken:

- Complexe systeemintegraties: Beheren van complexe integraties met andere systemen en platforms na overleg met de ICT-afdeling van DHS.
- Beleidsontwikkeling: Ontwikkelen en implementeren van bedrijfsbrede beleidslijnen en procedures voor het gebruik van Microsoft 365 op afroep van DHS.
- Compliance en beveiligingsbeleid: Zorgen voor naleving van regelgeving en implementeren van geavanceerde beveiligingsbeleid.
- Performance monitoring en optimalisatie: Monitoren van de systeemprestaties en optimaliseren voor maximale efficiëntie.
- Advies en strategie: Adviseren over toekomstige technologische ontwikkelingen en strategieën voor het gebruik van Microsoft 365 binnen de organisatie op afroep van DHS.

3.8. Google Cloud

1e-lijns Google Cloud Beheer

Verantwoordelijkheid:
Basisgebruikersondersteuning en probleemoplossing voor Google Cloud- diensten.

Taken:

- Gebruikersvragen: Aannemen en registreren van vragen over Google Cloud- toepassingen, met name van leerlingen en onderwijspersoneel.
- Basisprobleemoplossing: Oplossen van eenvoudige problemen zoals inlogproblemen, basisfunctionaliteiten van Google Workspace-apps (voorheen G Suite) zoals Gmail, Docs, Classroom.
- Gebruikersaccounts: Wachtwoord resets.
- Documentatie en Richtlijnen: Verstrekken van handleidingen en instructies voor standaardgebruik van Google Clouddiensten.
- Escalatie: Doorsturen van complexere vragen of problemen naar de 2e-lijns ondersteuning.

2e-lijns Google Cloud Beheer

Verantwoordelijkheid
Geavanceerde technische ondersteuning en configuratie van Google Cloud- diensten voor onderwijsdoeleinden. Changes kunnen na een CAB overleg worden doorgevoerd.

Taken:

- Geavanceerde probleemoplossing: Aanpakken van complexere problemen die betrekking hebben op Google Cloud-apps en -diensten.
- Beheer van Gebruikersrechten en Toegang: Configureren van toegangsrechten en gebruikersrechten voor leerlingen en personeel.
- Applicatie- en Dienstenconfiguratie: Beheren van instellingen voor specifieke Google Cloudapplicaties, inclusief Classroom en andere onderwijstools.
- Beveiligingsbeheer: Monitoren en verbeteren van de beveiligingsinstellingen binnen de Google Cloud-omgeving.
- Data Management: Beheren van data en privacy-instellingen conform onderwijsnormen en regelgeving.

3e-lijns Google Cloud Beheer

Verantwoordelijkheid
Expertondersteuning voor complexe integraties, beleidsontwikkeling en strategisch beheer van Google Clouddiensten in een onderwijsomgeving. Changes kunnen na een CAB overleg worden doorgevoerd.

Taken:

- Complexe Systeemintegraties: Beheren van integraties tussen Google Cloud en andere onderwijssystemen of platforms.
- Beleidsontwikkeling: Ontwikkelen van strategieën en beleid voor het effectief gebruik van Google Cloud binnen de onderwijsinstelling.
- Compliance en Beveiligingsbeleid: Zorgen voor naleving van onderwijsgerichte regelgeving en het implementeren van geavanceerd beveiligingsbeleid.
- Performance Monitoring en Optimalisatie: Toezicht houden op de systeemprestaties en optimalisatie voor onderwijsdoeleinden.
- Strategische Advisering: Adviseren over technologische ontwikkelingen en toekomstige implementatiestrategieën van Google Cloud in het onderwijs.

3.9. Beheer Apple Devices

1e-lijns Beheer van Apple Devices met JAMF, Microsoft Intune en Apple beheer- omgeving
Basisgebruikersondersteuning en probleemoplossing voor Apple-apparaten beheerd via JAMF, Microsoft Intune of Apple beheer-omgeving.

Verantwoordelijkheid
Basisgebruikersondersteuning en probleemoplossing voor Apple devices.

Taken:

- Gebruikersvragen: Aannemen en registreren van vragen gerelateerd aan het gebruik van Apple-apparaten.
- Basisprobleemoplossing: Assisteren bij veelvoorkomende problemen zoals connectiviteitsissues, app-installaties, en basisfuncties van het apparaat.
- Documentatie en Richtlijnen: Verstrekken van handleidingen en instructies voor standaardgebruik van Apple-apparaten onder beheer van Intune of Apple beheer-omgeving.
- Accountbeheer: Assisteren bij basisaccountmanagement zoals inlogproblemen, maar zonder wijzigingen in beveiligingsbeleid of apparaat configuratie.
- Escalatie: Doorverwijzen van complexere problemen of configuratieverzoeken naar de 2e-lijns ondersteuning.

2e-lijns Beheer van Apple Devices met Microsoft Intune en Apple beheer-omgeving

Verantwoordelijkheid
Geavanceerde technische ondersteuning en apparaat configuratie. Changes kunnen na een CAB overleg worden doorgevoerd.

Taken:

- Geavanceerde probleemoplossing: Aanpakken van complexere technische problemen die specifiek zijn voor Apple-apparaten.
- Apparaatconfiguratie: Aanpassen van apparaatinstellingen via JAMF, Intune en beheeromgeving Apple, inclusief beveiligingsbeleid, applicatiebeheer, en Wifi- instellingen.
- Beveiligingsbeheer: Monitoren en toepassen van beveiligingsupdates en -patches.
- Applicatiebeheer: Beheren en troubleshooten van applicaties gedistribueerd via Intune.
- Compliance en Beleid: Zorgen voor naleving van interne beleidslijnen en beveiligingsstandaarden op Apple-apparaten.

3e-lijns Beheer van Apple Devices met Microsoft Intune en Apple beheer-omgeving

Verantwoordelijkheid
Specialistische ondersteuning voor complexe vraagstukken en strategisch apparaat beheer. Changes kunnen na een CAB overleg worden doorgevoerd.

Taken:

- Complexe Systeemintegraties: Beheren van geavanceerde integraties tussen Apple-apparaten, Microsoft Intune, en andere bedrijfssystemen.
- Beleidsontwikkeling: Ontwikkelen van geavanceerde beheerstrategieën en beleid voor het gebruik van Apple-apparaten binnen de organisatie.
- Hoogwaardige Technische Ondersteuning: Oplossen van zeer complexe technische problemen en verstrekken van diepgaande technische expertise.
- Strategische Advisering: Adviseren over de implementatie van nieuwe technologieën en beheerbenaderingen voor Apple-apparaten.
- Performance Monitoring en Optimalisatie: Analyseren en optimaliseren van de prestaties van Apple-apparaten binnen de bedrijfsomgeving.

3.10. Applicatieleveranciers (AFAS/Esis etc.)

1e-lijns Applicatieleveranciers

Verantwoordelijkheid
Basisgebruikersondersteuning en voorziet melding van extra informatie voor de functioneel applicatie beheerder van DHS.

Taken:

- Gebruikersondersteuning: Beantwoorden van basisvragen over het gebruik van de applicaties (AFAS, Esis, etc.).
- Incidentregistratie: Registreren van problemen en verstoringen gemeld door gebruikers.
- Gebruikershandleidingen: Verstrekken van basisgebruikershandleidingen en documentatie.
- Meldingen: Voorziet de melding van extra informatie zodat de SPoC dit kan doorzetten naar de Functioneel applicatie beheerder voor opvolging.

3.11. Presentatiemiddelen

1e-lijns Beheer van Presentatiemiddelen

Verantwoordelijkheid
Basisgebruikersondersteuning en probleemoplossing voor presentatiemiddelen. Met presentatiemiddelen bedoelen we projectoren, interactieve whiteboards, en audiovisuele systemen (hier wordt geen Microsoft Teams mee bedoeld)

Taken:

- Gebruikersvragen: Aannemen en registreren van vragen gerelateerd aan het gebruik van presentatiemiddelen.
- Basisprobleemoplossing: Assisteren bij veelvoorkomende problemen zoals connectiviteitsissues, basisinstellingen van apparatuur, en assistentie bij het gebruik van standaardpresentatietools.
- Documentatie: Verstrekken van handleidingen en instructies voor standaardgebruik van presentatiemiddelen.

- Escalatie: Doorverwijzen van complexere technische problemen of specifieke configuratieverzoeken naar de 2e-lijns ondersteuning.

2e-lijns Beheer van Presentatiemiddelen

Verantwoordelijkheid
Geavanceerde technische ondersteuning en configuratie van presentatiemiddelen.

Taken:

- Geavanceerde probleemoplossing: Aanpakken van complexere technische problemen die betrekking hebben op presentatiemiddelen.
- Apparatuur configuratie: Configureren en aanpassen van instellingen van vaste en draagbare presentatiemiddelen.
- Beheer van Software: Installeren en updaten van software die nodig is voor de bediening en aansturing van presentatiemiddelen, zoals presentatiesoftware of drivers op de beheerde systemen (leerkracht devices).

3.12. Printing (Afdrukken)

1e-lijns Beheer van Printing (Afdrukken), multifunctionals en printers

Verantwoordelijkheid
Basisgebruikersondersteuning en eenvoudige probleemoplossing voor print gerelateerde zaken.

Taken:

- Gebruikersvragen: Aannemen en registreren van gebruikersvragen gerelateerd aan printproblemen.
- Basisprobleemoplossing: Helpen bij veelvoorkomende printproblemen zoals papierstoringen, cartridge vervangen
- Printopdrachten Beheren: Assisteren bij het versturen of annuleren van printopdrachten.
- Documentatie: Verstrekken van handleidingen en instructies voor standaard printtaken en -probleemoplossingen.
- Escalatie: Verzamelen van extra informatie zodat de SPoC de melding kan escaleren bij de beheerder van de online printing omgeving (Canon).
- (Her)Uitrol Uniflow client software werkplekken (intune)
- Installatie van dedicated printers op werkplekken

2e-lijns Beheer van Printing (Afdrukken), multifunctionals en printers
Geavanceerde technische ondersteuning en beheer van de online printing omgeving (uniflow).

Taken:

- Uniflow: Inrichting uniflow configuraties en koppelingen
- Updaten client software en distributie klaarmaken in intune.
- Printbeleid en -rechten: Beheren van printbeleid, gebruikersrechten en toegangscontroles voor printservices.
- Printerconfiguratie: Configureren en aanpassen van instellingen van printers, inclusief netwerkprinters en multifunctionele apparaten.

3.13. Identity and Access Management (IAM)

1e-lijns Beheer van IAM (Identity and Access Management)

Verantwoordelijkheid
Basisondersteuning voor gebruikersvragen en toegangsproblemen.

Taken:

- Gebruikersvragen en -problemen: Registreren en doorgeven van gebruikersvragen over toegangsproblemen en rechten.
- Basishulp bij Toegangsproblemen: Assisteren van gebruikers bij het verkrijgen van toegang tot systemen, zoals het begeleiden bij het resetten van wachtwoorden.
- Documentatie: Verstrekken van handleidingen en instructies voor standaard IAM- taken en -probleemoplossingen.
- Escalatie: Doorverwijzen van complexere problemen of verzoeken naar 2e-lijns ondersteuning.

2e-lijns Beheer van IAM (Identity and Access Management)

Verantwoordelijkheid
Geavanceerde technische ondersteuning en beheer van identiteits- en toegangsrechten. veranderingen in de IAM, nieuwe of aanpassingen in bestaande koppelingen hebben een CAB nodig voor implementatie.

Taken:

- Beheer van Toegangsrechten: Configureren en beheren van gebruikersrechten en toegangscontroles in verschillende systemen.
- Probleemoplossing: Oplossen van complexere toegangs- en authenticatieproblemen.

- Beleid en Procedures: Ontwikkelen en toepassen van IAM-beleid en -procedures, indien DHS dit wenst.
- Integratie en Testen: Zorgen voor integratie van IAM-oplossingen met andere systemen en applicaties.
- Monitoring en Analyse: Monitoren en analyseren van toegangslogs en beveiligingswaarschuwingen.

3e-lijns Beheer van IAM (Identity and Access Management)

Verantwoordelijkheid
Specialistische ondersteuning, ontwikkeling en strategisch beheer van IAM- oplossingen. Voor veranderingen aan de IAM is een CAB noodzakelijk,

Taken:

- Complex Systeembeheer: Beheren en optimaliseren van geavanceerde IAM- oplossingen en -platformen.
- Beleidsontwikkeling: Ontwikkelen van strategieën en beleid voor IAM, inclusief compliance en regelgeving.
- Technische Expertise: Bieden van diepgaande technische expertise voor complexe IAM-vraagstukken.
- Strategische Planning: Adviseren over de implementatie van nieuwe IAM- technologieën en best practices.
- Risicobeheer: Identificeren en beheren van risico's gerelateerd aan identiteits- en toegangsbeheer.

3.14. Security (Beveiliging)

1e-lijns Beheer van Security (Beveiliging)

Verantwoordelijkheid
Basisondersteuning voor gebruikersvragen en eenvoudige beveiligingsproblemen.

Taken:

- Gebruikersvragen: Registreren en doorgeven van gebruikersvragen en -meldingen over beveiligingsproblemen.
- Basisprobleemoplossing: Assisteren bij veelvoorkomende beveiligingsvragen, zoals het begeleiden bij het resetten van wachtwoorden of het melden van verdachte e- mails.
- Incidentregistratie: Registreren van beveiligingsincidenten en doorgeven aan de relevante 2e-lijnsteams voor verdere analyse.

- Escalatie: Doorverwijzen van complexere beveiligingsproblemen of -verzoeken naar de 2e-lijns ondersteuning.

2e-lijns Beheer van Security (Beveiliging)

Verantwoordelijkheid
Geavanceerde technische ondersteuning en beheer van de beveiligingsinfrastructuur.

Taken:

- Incidentbeheer: Diepgaande analyse en respons op beveiligingsincidenten samen met de privacy officer en CISO van DHS.
- Adviseren: Adviseren bij het Beveiligen van onze ICT omgeving: Adviseert de SICO bij het verbeteren van de beveiliging van onze ICT omgeving indien DHS dit wenst.
- Risicoanalyse: Uitvoeren van risicoanalyses en beveiligingsaudits.
- Bewustmakingscampagnes: Helpt de privacy officer en CISO van DHS bij het opzetten van een beveiligingsbewustzijn campagne indien DHS dit wenst.

3e-lijns Beheer van Security (Beveiliging)

Verantwoordelijkheid
Specialistische ondersteuning, strategische planning en beheer van complexe beveiligingsvraagstukken.

Taken:

- Geavanceerde Incidentrespons: Coördineren en leiden van de respons op complexe en geavanceerde beveiligingsincidenten.
- Beleidsontwikkeling en Compliance: Helpt bij het ontwikkelen van geavanceerde beveiligingsstrategieën, beleid en zorgen voor naleving van regelgeving en standaarden.
- Technologische Innovatie: Op verzoek van DHS wordt bij nieuwe beveiligingstechnologieën een CAB-voorstel opgesteld ter besluitvorming over implementatie.
- Strategisch Risicobeheer: Identificeren, analyseren en beheren van strategische beveiligingsrisico's