Bijlage G – Beleid Change Management

Inleiding

De rollen binnen het change management proces zijn op de volgende manier verdeeld:

Eindverantwoordelijk: IT-manager.

Uitvoerend:

- Helpdesk: Zij zijn het eerste aanspreekpunt voor wijzigingen en beoordelen of het gaat om een standaard change of een change voor het CAB.
- Functioneel beheer: Uitvoerend, adviserend en meewerkend in het wijzigingsproces
- CAB: Coordinator informatiemanagement, Enterprise Architect, Coördinator IT Beheer, Information Security Officer, Privacy Officer.
- Leveranciers: Wanneer het een wijziging betreft, die onder het beheer zit van een leverancier, dan wordt de wijziging uitbesteed aan deze leverancier. Met de leveranciers zijn van tevoren afspraken gemaakt in de vorm van een beheerovereenkomst en/of SLA. Indien de wijziging niet onder het beheer zit van een leverancier, dan wordt de wijziging uitgevoerd door (de opdrachtnemer voor) IT-Beheer.

BIO-controls

Change management moet voldoen aan de volgende BIO-controls:

- Controlnummer 12.1.2 Wijzigingsbeheer:
  Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.

- Controlnummer 12.2.1 Bescherming tegen malware:
  Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.

Doel

Om conformiteit met beheersmaatregel 12.1.2 te borgen, moeten we als organisatie het volgende realiseren:

- Wijzigingen in informatie verwerkende faciliteiten en informatiesystemen zijn onderworpen aan procedures voor wijzigingsbeheer.

Streven is dat alle software en systemen altijd worden bijgewerkt naar de nieuwste versie, met een maximale afwijking van één versie ten opzichte van de meest recente release.

Wijzigingsbeheer richt zich op het effectief doorvoeren van wijzigingen met minimale verstoring van de dienstverlening en blijvende naleving van functionele en beveiligingseisen. Dit omvat:

- Definiëren en toewijzen van verantwoordelijkheden.
- Vaststellen van regels en procedures.

- Het doel van patchmanagement is tweeledig:

- het is gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur,
- op een zo efficiënt mogelijk wijze met zo min mogelijk verstoringen stabiele (veilige) systemen te creëren.

Uitgangspunten

Bij hWh onderscheiden we de volgende soorten IT-wijzigingen:

- **Standaardwijzigingen:** Dit zijn vooraf goedgekeurde wijzigingen die een lage impact hebben, eerder uitgevoerd zijn, en meestal gedocumenteerd zijn. Standaardwijzigingen vereisen alleen een risicobeoordeling en goedkeuring wanneer ze voor de eerste keer worden geïmplementeerd. Daarna kunnen ze zonder risicobeoordeling plaatsvinden.
- **Niet-standaardwijzigingen:** een niet-standaardwijziging moet het gehele wijzigingsproces doorlopen. De wijziging moet worden gepland, het risico moet worden beoordeeld en de wijziging moet worden goedgekeurd.
- **Spoedwijzigingen:** Dit zijn niet-standaardwijzigingen met een hoge urgentie, waarbij versnelde beoordeling, goedkeuring en implementatie is vereist is. Denk bijvoorbeeld aan het installeren van een noodpatch voor een kwetsbaarheid in de beveiliging.
  Spoedwijzigingen dienen onverwijld te worden geïnstalleerd.
- **Patches:** Dit zijn doorgaans kleine programma's die aanpassingen maken om fouten op te lossen of verbeteringen aan te brengen in bestaande IT-omgeving. Ieder systeem of apparaat dat software bevat en aan een netwerk gekoppeld is, is in principe onderhevig aan patchmanagent.
  Een patch is een standaardwijziging. Patches dienen binnen 7 dagen na release te worden geïnstalleerd.
- **Update:** Dit is een kleine wijziging of verbetering aan een bestaand softwareprogramma of systeem. Updates worden uitgebracht om bugs te verhelpen, beveiligingsproblemen op te lossen of kleine verbeteringen aan te brengen.
  Voorbeelden van updates zijn:
  - **Beveiligingspatches**: Kleine updates die beveiligingslekken dichten.
  - **Bugfixes**: Oplossingen voor fouten die in de software zijn gevonden.
  - **Kleine verbeteringen**: Bijvoorbeeld het toevoegen van een nieuwe functie of het verbeteren van de prestaties.

  Een update is een standaardwijziging. Updates dienen binnen 7 dagen na release te worden geïnstalleerd.
- **Upgrade:** Dit is een grotere, meer ingrijpende verandering aan software of hardware. Upgrades brengen vaak nieuwe functies, aanzienlijke verbeteringen en soms een geheel nieuwe gebruikersinterface met zich mee. Voorbeelden van upgrades zijn:
  - **Nieuwe softwareversies**: Bijvoorbeeld het overstappen van Windows 10 naar Windows 11.
  - **Grote softwareverbeteringen**: Bijvoorbeeld een nieuwe versie van een grafisch ontwerpprogramma met veel nieuwe functies.

  Een upgrade is een standaardwijziging. Upgrades dienen binnen 90 dagen na release te worden geïnstalleerd.

Afhandeling van wijzigingen

Bij de afhandeling van wijzigingen spelen de volgende aspecten een rol:

1. **Risicobeheer**: Identificeren, classificeren en mitigeren van potentiële risico's die gepaard gaan met veranderingen om negatieve gevolgen te minimaliseren, onder andere door zaken eerst in een afgeschermde omgeving of beperkt uit te rollen.
2. **Continuïteit**: Zorgen dat de dagelijkse bedrijfsvoering zo min mogelijk wordt verstoord door veranderingen.
3. **Kwaliteitsverbetering**: Verbeteren van processen, systemen en diensten door gecontroleerde en geplande veranderingen.
4. **Transparantie**: Creëren van een duidelijk en gedocumenteerd proces voor het aanvragen, beoordelen, goedkeuren en implementeren van veranderingen.
5. **Betrokkenheid**: Betrekken van alle relevante stakeholders bij het veranderingsproces om draagvlak en acceptatie te vergroten.
6. **Efficiëntie**: Optimaliseren van de middelen en tijd die nodig zijn om veranderingen door te voeren.
7. **Compliance**: Zorgen dat veranderingen voldoen aan interne beleidsregels en externe regelgeving.

Om deze aspecten te borgen zijn er afhankelijk van de aard en impact van de wijziging, verschillende manieren om de wijziging af te handelen:

- Directe afhandeling door servicedesk of functioneel beheer;
- Behandeling van de wijziging door het CAB, en afhankelijk van de uitkomst:
    - Afhandeling door functioneel beheer / leverancier / opdrachtnemer IT-beheer;
    - Afhandeling als IT-project.

Afhandeling van de wijziging omvat in alle gevallen:

- Doorvoeren van de benodigde technische aanpassing;
- Communicatie met eindgebruikers, vooraf, tijdens en achteraf;
- Documenteren van de wijziging;
- Aanpassen van documentatie en trainingsmateriaal.