Spinware Solutions B.V.
veilig werken met de cloud

Incidentenbeleid

Versie: augustus 2024

Inhoudsopgave

1. Inleiding

Dit incidentenbeleid is opgesteld om een gestructureerde aanpak te bieden voor het beheren en oplossen van incidenten die zich kunnen voordoen bij het leveren van ICT-diensten aan de klanten van Spinware Solutions. Dit beleid beschrijft de procedures en verantwoordelijkheden om ervoor te zorgen dat incidenten effectief en efficiënt worden afgehandeld, met minimale verstoring van de dienstverlening.

1.1. Doelstellingen

De doelstellingen van dit incidentenbeleid zijn:

- **Snelle identificatie en oplossing** van incidenten om de impact op de dienstverlening te minimaliseren.
- **Duidelijke communicatie** met klanten tijdens het incidentbeheerproces.
- **Preventieve maatregelen** nemen om herhaling van incidenten te voorkomen.
- **Continue verbetering** van het incidentbeheerproces door middel van evaluatie en aanpassing.

1.2. Definities

- **Incident**: Een onvoorziene gebeurtenis die de normale werking van een dienst verstoort of dreigt te verstoren.
- **Impact**: De mate waarin een incident de bedrijfsvoering van de klant beïnvloedt.
- **Urgentie**: De snelheid waarmee een incident moet worden opgelost om verdere schade te voorkomen.
- **Prioriteit**: De classificatie van een incident op basis van impact en urgentie.

1.3. Incidentclassificatie

Incidenten worden geclassificeerd op basis van hun impact en urgentie:

- **Kritieke incidenten (Prioriteit 1)**: Incidenten met een hoge impact en urgentie die onmiddellijke aandacht vereisen, zoals een volledige netwerkuitval.
- **Hoge Prioriteit incidenten (Prioriteit 2):** Incidenten met hoge impact maar lagere urgentie, zoals een serverstoring die echter redundante systemen heeft.
- **Middelmatige Prioriteit incidenten (Prioriteit 3)**: Incidenten met gemiddelde impact en urgentie, zoals problemen met bepaalde softwarefunctionaliteiten.
- **Lage Prioriteit incidenten (Prioriteit 4):** Incidenten met lage impact en urgentie, zoals kleine bugs of gebruikersondersteuning.

In het volgende hoofdstuk bespreken we het incidentbeheer proces van Spinware Solutions.

2. Incidentbeheer proces

Het incidentbeheerproces bij Spinware Solutions bestaat uit de volgende stappen:

1. **Melding van een incident**
    - Incidenten kunnen door klanten worden gemeld via e-mail of telefoon.
    - Bij ontvangst van een incidentmelding wordt een taak aangemaakt.
    - De eerstelijns support registreert de details van het incident, inclusief de symptomen, de betrokken systemen en de contactgegevens van de melder.
2. **Classificatie en prioritering**
    - Het incident wordt beoordeeld en geclassificeerd op basis van impact en urgentie.
    - Een prioriteit wordt toegekend volgens de classificatiecriteria.
3. **Toewijzing en eerste analyse**
    - Het incident wordt toegewezen aan een geschikt team of specialist voor eerste analyse.
    - De eerste analyse omvat het identificeren van de oorzaak en het inschatten van de benodigde middelen voor de oplossing.
4. **Oplossen van het incident**
    - Er wordt een actieplan opgesteld en uitgevoerd om het incident op te lossen.
    - De voortgang wordt gedocumenteerd en de klant wordt regelmatig geïnformeerd over de status van het incident.
    - Bij complexe of langdurige incidenten worden extra resources ingezet en wordt er nauw samengewerkt met externe leveranciers indien nodig.
5. **Incidentafsluiting**
    - Na het oplossen van het incident wordt een sluitingscontrole uitgevoerd om te bevestigen dat de dienstverlening is hersteld.
    - De taak wordt gesloten en gedocumenteerd; inclusief een volledige beschrijving van het incident, de oorzaak, de genomen maatregelen en de uiteindelijke oplossing
    - Feedback van de klant wordt verzameld om de kwaliteit van de oplossing en de tevredenheid te beoordelen.
6. **Post-incident review**
    - Een evaluatie van het incident wordt uitgevoerd om de oorzaak en het oplossingsproces te beoordelen.
    - Er worden aanbevelingen gedaan voor verbeteringen om toekomstige incidenten te voorkomen.
    - De bevindingen worden gedeeld met relevante stakeholders en de geleerde lessen worden geïntegreerd in het continue verbeteringsproces.

2.1. Communicatie

Tijdens het incident wordt de klant op de hoogte gehouden van de status en voortgang van het incident door middel van regelmatige updates. Voor kritieke incidenten worden klanten direct telefonisch geïnformeerd naast de gebruikelijke meldingsmethoden.

Wanneer het incident is afgesloten volgt een samenvatting van het incident, inclusief de oorzaak, oplossing en eventuele preventieve maatregelen. Dit wordt aan de klant verstrekt.

2.2. Rollen en verantwoordelijkheden

- Incidentbeheerder: Verantwoordelijk voor de algehele coördinatie van het incidentbeheerproces.
- Technische specialisten: Verantwoordelijk voor de technische analyse en oplossing van incidenten.
- Communicatiebeheerder: Verantwoordelijk voor de communicatie met klanten tijdens incidenten.

2.3. Training en bewustzijn

Alle medewerkers worden regelmatig getraind in incidentbeheerprocedures en best practices. Er worden simulaties en oefeningen gehouden om de effectiviteit van het incidentbeheerproces te testen en te verbeteren.

2.4. Rapportage en analyse

Er worden regelmatig incidentrapportages opgesteld en geanalyseerd om trends en patronen te identificeren. De bevindingen uit de analyses worden gebruikt om het incidentbeheerproces continu te verbeteren.

2.5. Naleving en evaluatie

Dit incidentenbeleid wordt jaarlijks geëvalueerd en, indien nodig, bijgewerkt om te voldoen aan veranderende omstandigheden en best practices. Feedback van klanten en medewerkers wordt gebruikt om het beleid en de procedures verder te verfijnen.

3. Conclusie

Door een gestructureerde en proactieve benadering van incidentbeheer te hanteren, streeft Spinware Solutions ernaar om de impact van incidenten op onze klanten te minimaliseren en een hoge kwaliteit van dienstverlening te waarborgen.

De medewerkers van Spinware Solutions zijn toegewijd aan continue verbetering en klanttevredenheid, en waarderen de samenwerking en feedback van onze klanten om deze doelen te bereiken.

Voor verdere vragen of meldingen van incidenten kunt u contact met ons opnemen met Rudolf Philipse via 070 3115400. Wij staan altijd klaar om u te ondersteunen en te zorgen voor een snelle en effectieve oplossing van eventuele problemen.

Bijlage I: Voorbeeldincident

Scenario: De server in het externe datacenter van Spinware Solutions is niet benaderbaar.

Incidentbeheerproces:

1. **Melding van het incident**
    - **Ontvangst**: Een klant meldt telefonisch dat hun diensten niet beschikbaar zijn. Het supportteam ontvangt de melding en maakt een taak aan.
    - **Registratie**: De supportmedewerker registreert de details van het incident, zoals de symptomen (onbereikbare server), betrokken systemen en contactgegevens van de melder.
2. **Classificatie en prioritering**
    - **Beoordeling**: Het incident wordt beoordeeld op basis van de impact (alle diensten zijn niet beschikbaar) en urgentie (kritiek voor bedrijfsvoering van de klant).
    - **Prioriteit**: Dit incident wordt geclassificeerd als een Kritiek incident (Prioriteit 1) vanwege de hoge impact en urgentie.
3. **Toewijzing en eerste analyse**
    - **Toewijzing**: Het incident wordt onmiddellijk toegewezen aan het netwerk- en serverbeheerteam.
    - **Eerste analyse**:
        i. Het team voert een eerste diagnose uit door te controleren of er netwerkconnectiviteit is met het datacenter.
        ii. Er wordt gecontroleerd of er een algemene storing is gemeld door het datacenter.
        iii. Het team probeert de server op afstand te herstarten via beschikbare beheertools.
4. **Oplossen van het Incident**
    - **Actieplan**:
        i. Als de eerste analyse aangeeft dat de server offline is, wordt er een technicus naar het datacenter gestuurd om fysieke toegang tot de server te verkrijgen.
        ii. De technicus controleert de hardware-status van de server, herstart de server indien nodig, en voert een uitgebreide diagnose uit.
    - **Communicatie**:
        i. Klanten worden elke 30 minuten op de hoogte gehouden van de voortgang via e-mail en telefoon.
        ii. Bij terugkeer naar operationele status worden klanten onmiddellijk geïnformeerd.
    - **Herstelmaatregelen**:
        i. Indien een hardware-probleem wordt gevonden, wordt vervangende hardware geïnstalleerd.
        ii. Softwarematige problemen worden opgelost door het herinstalleren of updaten van de serversoftware.
5. **Incidentafsluiting**
    - **Sluitingscontrole**:

i. Na het oplossen van het probleem, wordt een sluitingscontrole uitgevoerd om te verifiëren dat alle diensten weer operationeel zijn.
ii. De klant bevestigt dat de dienst naar behoren functioneert.

- **Documentatie**:
  i. Het incidentticket wordt bijgewerkt met een volledige beschrijving van het incident, de oorzaak, de genomen maatregelen en de uiteindelijke oplossing.
  ii. Het ticket wordt gesloten en een samenvatting wordt naar de klant gestuurd.

6. **Post-Incident review**
   - **Evaluatie**:
     i. Een evaluatie van het incident wordt uitgevoerd om de oorzaak en het oplossingsproces te beoordelen.
     ii. Het team bespreekt de effectiviteit van de respons en identificeert verbeterpunten.
   - **Preventieve maatregelen**:
     i. Aanbevelingen worden gedaan voor verbeteringen, zoals het upgraden van monitoringtools, trainen van personeel, of aanpassingen aan de infrastructuur.
   - **Verslaglegging**:
     i. Een gedetailleerd incidentrapport wordt opgesteld en gedeeld met relevante stakeholders.