# Bijlage E BIV-classificatie VfPf

## Behorende bij de aanbesteding voor een *Inkoop- en contractmanagementtool (ref 2023.004)*

De kwaliteitsaspecten die worden toegepast op informatiebeveiliging zijn Beschikbaarheid, Integriteit, en Vertrouwelijkheid. Deze termen worden hier inclusief de deelaspecten beschreven. Alle aspecten kunnen worden geclassificeerd in laag, midden en hoog.

Beschikbaarheid:
Het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.

**Deelaspecten hiervan zijn:**
- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Voor de beschikbaarheid komt de classificatie ***midden(2)***

Integriteit:
Het waarborgen van de juistheid en de volledigheid van informatie en verwerking.

**Deelaspecten hiervan zijn:**
- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Voor de integriteit komt de classificatie ***midden(2)***

Vertrouwelijkheid:
Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe is geautoriseerd.

**Deelaspecten hiervan zijn:**
- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Voor de vertrouwelijkheid komt de classificatie ***hoog(3)***

De BIV classificatie matrix is als volgt:

| Bron | Ref. nr. | Uitgangspunten: |
|---|---|---|
| | **Op basis van een BIV classificatie Midden 2-Midden 2- Hoog 3 stelt VfPf als mitigerende maatregelen de volgende voorwaarden aan de dienstverlening:** | |
| BIV Classificatie; B=1 | 1 | Er is een redundante architectuur geimplementeerd met behulp van een cold standby. |
| | 2 | 1 x per jaar wordt de backup en recovery procedure alswel de volledigheid en recovery van de backup zelf getest. |
| | 3 | Kopieen van Back-ups worden op een tweede/secundaire locatie bewaard in overeenstemming met de bewaartermijn van het origineel. |
| | 4 | De Fysieke omgeving van de IT apparatuur bevat maatregelen ter preventie, detectie en repressie van incidenten en calamiteiten zoals brand en wateroverlast. |
| | 5 | De secundaire locatie is op voldoende (smart maken) afstand van de primaire locatie en is vastgesteld op basis van een risicoanalyse. |
| | 6 | De verwachte belasting van de applicatie is laag, dit betekent een laag aantal gebruikers van gemiddeld(naar schatting 30 gebruikers). |
| | 7 | De applicatie dient gedurende kantooruren beschikbaar te zijn (7:00 - 23:00) |
| | 8 | Er zijn geen wettige verplichtigen m.v.t. de beschikbaarheid. |
| | 9 | Als de applicatie niet beschikbaar is zal dit niet leiden tot imagoverlies. |
| BIV Classificatie; B=2 | 10 | Er is geen sprake van een noodgeval als de data tijdelijk niet beschikbaar is. |
| BIV Classificatie; I=1 | 11 | Bewaar audit trails minstens 1 jaar online direct toegankelijk. |
| | 12 | Richt anitivirus/malware maatregelen in op servers van informatiesystemen. |
| | 13 | Het effect van fouten of ongeautoriseerde veranderingen in gegevens zijn intern. |
| | 14 | Fouten of ongeautoriseerde veranderingen leiden niet tot imagoverlies. |
| | 15 | Personen kunnen geen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van gegevens. |
| | 16 | Antivirus/malware maatregelen zijn aanwezig op werkstations en externe gateways om malware te detecteren en te verwijderen. |
| BIV Classificatie; I=2 | 17 | Alle acties die worden uitgevoerd door personen die Root of Admin (high privileged accounts) autorisaties worden gelogged. |
| | 18 | Er kunnen geen fouten of ongeautoriseerde veranderingen in de gegevens zitten(BIV is gemiddeld). |
| | 19 | Financiële fraude kan niet plaatsvinden door fouten in de gegevens of ongeautoriseerde wijzigingen. |
| BIV Classificatie; V=1 | 20 | Alle toegang tot audit trails wordt gelogged. |
| | 21 | Toegang tot de applicaties en fileshares (non-sensitive data) wordt verleend op basis van de rol van een gebruiker (rol management). |
| | 22 | Alle netwerkencomponenten, systemen, databases en middleware zijn gehardened. |
| | 23 | Default wachtwoorden van systemen, databases, middleware en applicaties zijn gewijzigd. |
| | 24 | Elke user heeft een persoonlijk account. |
| | 25 | Alle niet persoonlijke accounts zijn gekoppeld aan/ herleidbaar naar natuurlijke personen. |
| | 26 | Accounts met hoge privileges worden alleen gebruikt voor administratieve doeleinden. |
| | 27 | Inactieve accounts worden automatisch gedeactiveerd na 3 maanden inactiviteit en uiterlijk 1,5 jaar na deactivering permanent verwijderd. |
| | 28 | Uitgegeven 'normal'account en autorisaties worden elk half jaar gereviewed. |
| | 29 | Elk kwartaal worden high privileged accounts en autorisaties gereviewed. |
| | 30 | 1-factor authenticatie met een complex wachtwoord wordt toegepast [vereisten complex]. |
| | 31 | Na 3 foutieve inlogpogingen wordt een wachtwoord geblokkeerd. |
| | 32 | Screensaver wordt binnen 15 minuten geactiveerd. |
| | 33 | Wachtwoorden en authenticatie data worden versleuteld tijdens transmisie en opslag middels sterke encryptietechnieken (one-way encryptie en sterke sleutels). |
| | 34 | Logging van in- en uitloggen op het interne netwerk. |
| | 35 | Remote access gebruikt 2-factor authenticatie en versleutelde communicatie. |
| | 36 | Vulnerability scans (intern en extern) worden voor in beheername en vervolgens elke 6 maanden uitgevoerd. |
| | 37 | Alle data & media worden verwijderd of vernietigd conform. |
| | 38 | Alle data & nedia worden verwijderd of vernietigd conform de bir normen. |
| | 39 | Productie, test en ontwikkelnetwerken zijn gescheiden. |
| | 40 | Alle backups worden versleuteld opgeslagen. |
| BIV Classificatie; V=2 | 41 | Visueel is onderscheid in productie, acceptatie en ontwikkeling front end omgevingen. |
| | 42 | Autorisaties in applicaties worden toegekend op basis van 'need-to-know' en 'need-to-have'. |
| | 43 | Applicaties (incl. klantapplicaties) makken gebruik van verificatie van username en password (SSO) of 1-factor authenticatie. |
| | 44 | Alle data buiten VfPf wordt versleuteld opgeslagen en verstuurd. |
| | 45 | Network intrusion Detection dient aanwezig te zijn. |
| | 46 | Netwerkcomponenten die aan het externe netwerk zijn gekoppeld bevatten 2-factor authenticatie. |
| | 47 | Time-out van 15 minuten op de actieve connecties |
| | 48 | Alle software (maatwerk, pakket, SAAS) dienen te voldoen aan best practice beveiligingsrollen (bij OWASP) |
| | 49 | VfPf IT omgevingen dienen logisch te zijn gescheiden en van andere organisaties |
| | 50 | Elk jaar en na elke significante wijziging wordt een interne en externe penetratietest uitgevoerd. Indien nodig ook bij een groot incident. |
| | 51 | Risk based logging is geconfigureerd om toegang te loggen en monitoren. |
| BIV Classificatie; V=3 | 52 | Er wordt gebruik gemaakt van netwerk filtering en analyse maatregelen binnen de IT domeinen |
| | 53 | 2-factor authenticatie moet worden toegepast |
| | 54 | Deblokkeren van geblokkeerde account dient handmatig plaats te vinden. |
| | 55 | Alle data worden versleuteld opgeslagen |
| | 56 | Servers bevinden zich in een aparte beveiligde ruimte binnen het datacenter |
| | 57 | Alle gebruik van authenticatiemiddelen wordt gelogged |
| | 58 | Gedetecteerde extreme aantallen verkeerde inlogpogingen worden direct aan Security Management gemeld. |
| | 59 | Host based ISD dient geactiveerd te zijn |
| | 60 | Personen kunnen niet benadeeld worden indien een datalek plaatsvindt. Gegevens moeten worden opgeslagen conform AVG. |
| | 61 | De classificatie van gegevens is vertrouwelijk en wordt strict alleen binnen de organisatie gebruikt. |
| | 62 | Interne IT beheerders maken gebruik van een Stepping Stone server om toegang te krijgen tot de omgeving. |
| | | |