

Beschikbaarheid

Beschikbaarheid is gedefinieerd als 'eigenschappen van het geheel van ICT-diensten, systemen, componenten en gegevensdragers die van invloed zijn op de tijd dat het product of de dienst (en daarmee informatie) beschikbaar is voor de geautoriseerde gebruiker, op de momenten dat het beschikbaar moet zijn'. Beschikbaarheid wordt gemeten aan de hand van de Mean Time Between Failures (MTBF). Dit is de gemiddelde tijd tussen het herstel van het ene incident en het optreden van het volgende incident.

Beschikbaarheid	Belangrijk	Noodzakelijk	Essentieel
Werktijden	08:00 - 17:00 maandag t/n vrijdag behoudens algemeen erkende feestdagen	08:00 - 21:00 maandag t/n vrijdag behoudens algemeen erkende feestdagen	24 * 7 behoudens gepland onderhoud
Beschikbaarheid tijdens werktijd	min 99,6%	min 99,6%	min 99,9%
Beschikbaarheid buiten werktijd	min 96,1%	min 96,1%	N.V.T.
Mean Time Between Failures (MTBF)	min 100 dagen	min 100 dagen	min 200 dagen
Mean Time To Repair (MTTR)	max 4 uur	max 4 uur	max 4 uur
Maximaal aantal storingen van 3 minuten of korter	4x per maand	2x per maand	1x per maand
Maximaal aantal storingen van langer dan drie minuten	1x per maand	1x per 2 maanden	1x per half jaar

Eis, conform de uitkomst van de Cloud checklist:

Noodzakelijk;

De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schadetoebrengen.

Beschikbaarheid tijdens werktijd: minimaal 99,6%;

Beschikbaarheid buiten werktijd: minimaal 96,1%;

Mean time between failures: minimaal 100 dagen;

Mean time to repair: max 4 uur;

Maximaal aantal storingen van 3 minuten of korter: 2x per maand;

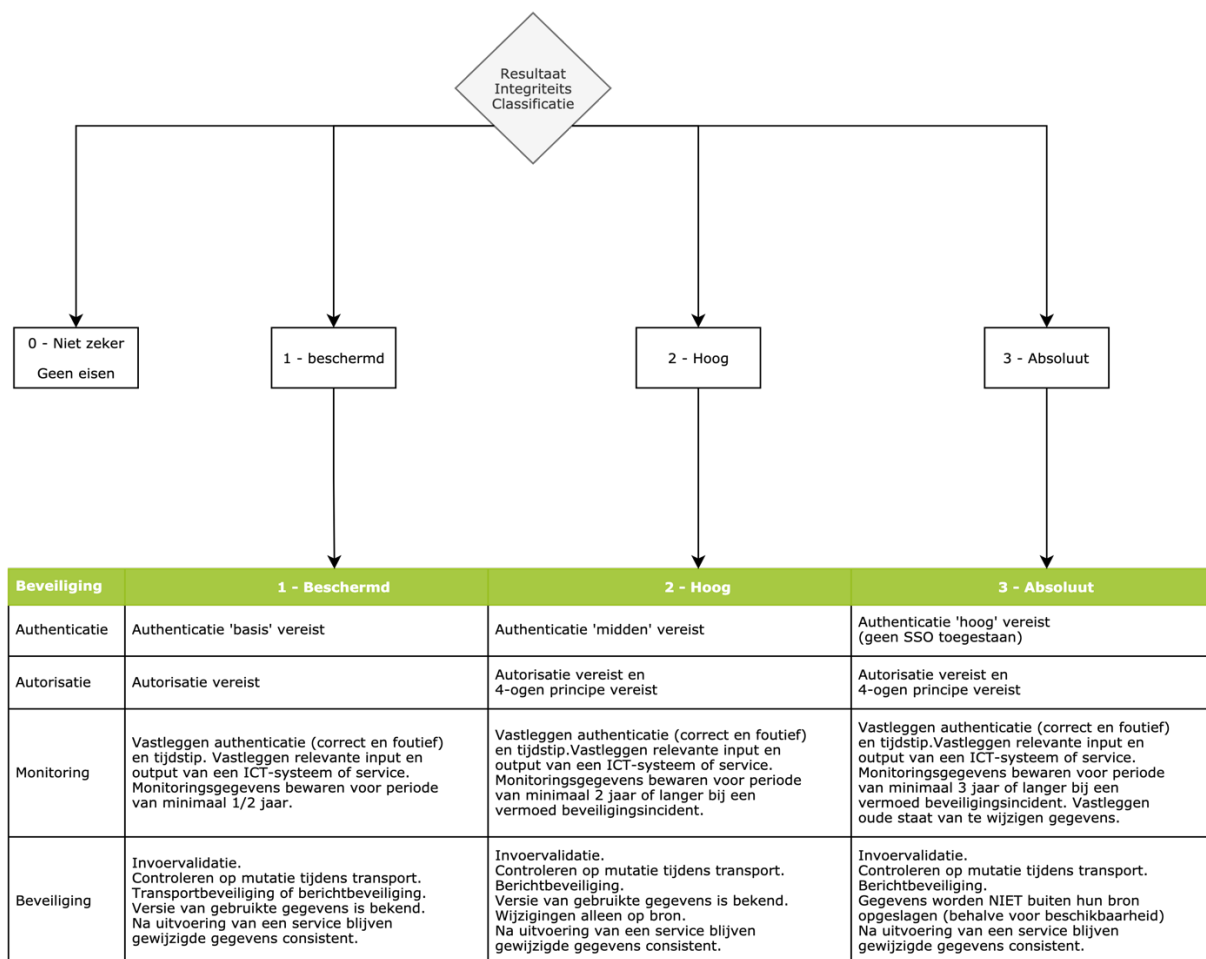
Maximaal aantal storingen van langer dan drie minuten: 1x per 2 maanden.

Integriteit

Het onderwerp integriteit valt normaliter in twee delen uiteen: de integriteit van datacommunicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het gemeentelijke proces zelf), en de integriteit van de informatie in de applicaties of fysiek (d.w.z. gerelateerd aan het gemeentelijke proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatie afhankelijk en afhankelijk van de eisen van een specifiek proces.

Voor de functionele integriteit van de informatievoorziening wordt een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Integriteit geeft de mate aan waarin de informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en tijdigheid van de transacties.



Integriteit eisen, conform de uitkomst van de Cloud checklist:

Hoog

Authenticatie: authenticatie 'midden (2FA)' vereist;

Autorisatie: autorisatie vereist en 4-ogen principe;

Monitoring:

- Vastleggen authenticatie (correct en foutief) en tijdstip.
- Vastleggen relevante input en output van een ICT-systeem of service.
- Monitoringsgegevens bewaren voor periode van minimaal 2 jaar of langer bij een vermoed beveiligingsincident.

Beveiliging:

- Invoervalidatie;
- Controleren op mutatie tijdens transport.

Berichtbeveiliging.

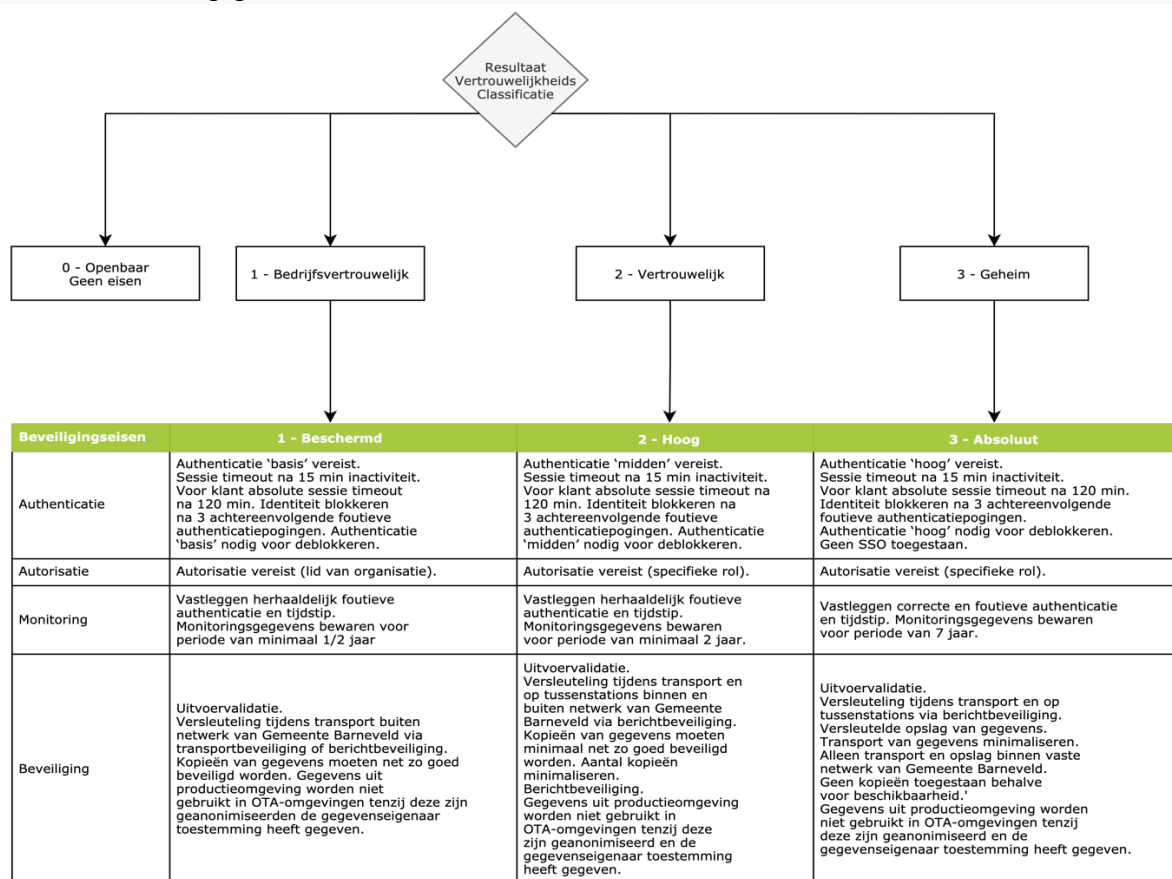
- Versie van gebruikte gegevens is bekend;
- Wijzigingen alleen op bron;
- Na uitvoering van een service blijven gewijzigde gegevens consistent.

Vertrouwelijkheid

Vertrouwelijkheid is het kwaliteitsbegrip waaronder privacybescherming maar ook de exclusiviteit van informatie gevangen kan worden. Het waarborgt dat alleen geautoriseerde toegang krijgen en dat informatie niet kan uitlekken.

Vertrouwelijke gegevens zijn bijvoorbeeld:

- Persoonsgegevens
- Gemeentelijke- en bedrijfsgeheimen
- Concurrentiegevoelige gegevens zoals voorbereidingen voor bestemmingsplannen
- Medische gegevens



Vertrouwelijk eisen, conform de uitkomst van de Cloud checklist:

Absoluut

Authenticatie:

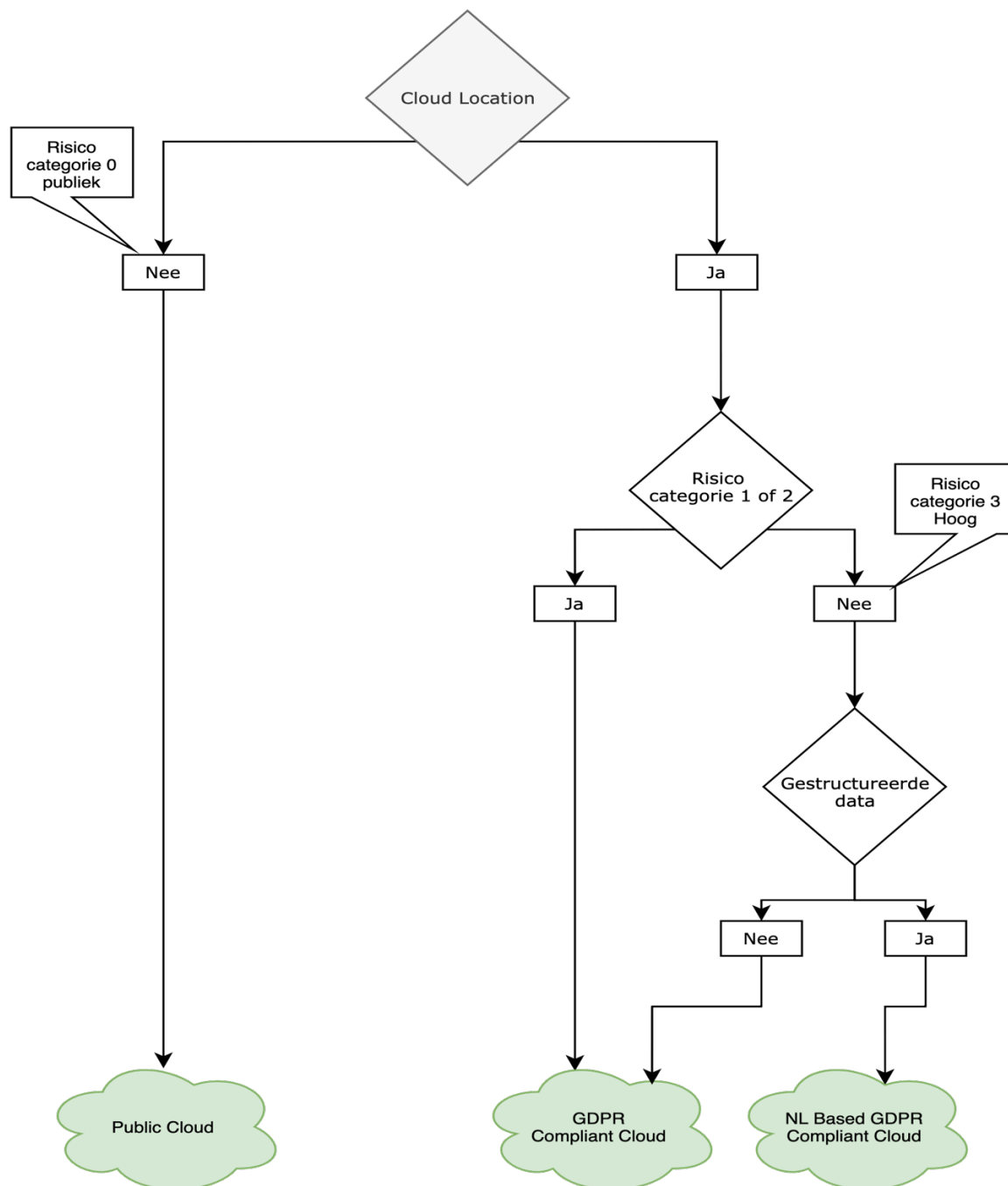
- Authenticatie 'hoog' vereist;
- Sessie timeout na 15 min inactiviteit;
- Absolute sessie timeout na 120 min;
- Identiteit blokkeren na 3 achtereenvolgende foutieve authenticatiepogingen;
- Authenticatie 'hoog' nodig voor deblokkeren, geen SSO toegestaan;
- Autorisatie vereist (specifieke rol).

Monitoring:

- Vastleggen correcte en foutieve authenticatie en tijdstip. Monitoringsgegevens bewaren voor periode van minimaal 7 jaar.

Uitvoervalidatie:

- Versleuteling tijdens transport en op tussenstations via berichtbeveiliging;
- Versleutelde opslag van gegevens;
- Transport van gegevens minimaliseren;
- Alleen transport en opslag binnen vaste netwerk van Gemeente Barneveld;
- Geen kopieën toegestaan behalve voor beschikbaarheid;
- Gegevens uit productieomgeving worden niet gebruikt in OTA-omgevingen tenzij deze zijn geanonimiseerd en de gegevenseigenaar toestemming heeft gegeven.



Eis, volgens uitkomst van de Cloud checklist:

Risicocategorie 3 (Hoog risico/geheim)

Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen

- Cloudprovider moet GDPR compliant zijn;
- Gestructureerde data zoals (databases, spreadsheets, applicatiedata etc.) mag alleen binnen Nederland gehost worden.