Versie: 1.0
Datum: 28 mei 2026
Opgesteld door: externe consultant, in opdracht van informatiebeveiligingscoordinator
Goedgekeurd door: Directie Brasholt Hekwerk BV

Table of Contents

Inleiding

Brasholt Hekwerk BV hecht grote waarde aan de beveiliging van informatie. In dit beleid wordt uitgelegd hoe Brasholt Hekwerk omgaat met informatiebeveiliging op basis van het CYRA Entry-Level raamwerk, dat een subset vormt van de ISO 27001 en ISO 27701 normen.

Het doel van dit beleid is om risico's te beperken, de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te borgen, en te voldoen aan relevante wet- en regelgeving, zoals de AVG en eisen gesteld door onze klanten.

> Deze template wordt onderhouden door Evelien Bras, the cyber partners. Voor aanvulling of verscherping, neem gerust contact op: e.bras@thecyberpartners.com

Toepassingsgebied (Scope)

Dit beleid geldt voor alle medewerkers, systemen, processen en gegevens van Brasholt Hekwerk BV die betrokken zijn bij de verwerking van bedrijfs- of persoonsgegevens, inclusief externe partijen en leveranciers indien van toepassing.

Governance & Rollen[1]

Rol	Verantwoordelijkheden
Directie	Goedkeuring beleid, toewijzen middelen, toezicht
Informatiebeveiligingscoördinator (IBC) (aan te wijzen door directie)	Beheer beleid, monitoring
HR manager (HR)	awareness
IT-Beheerder	Technische implementatie van beveiligingsmaatregelen
Functionaris Gegevensbescherming (FG)	Toezicht op privacymaatregelen en naleving AVG/ISO 27701
Alle medewerkers	Naleven van beleid en meldingsplicht bij incidenten

Wettelijke en contractuele kaders

- ISO 27001: Internationale norm voor informatiebeveiliging
- NIS2: Europese richtlijn voor netwerk- en informatiebeveiliging;
- AVG: Bescherming van persoonsgegevens;
- Nationale en sectorale wetgeving: Cyberbeveiligingswet

[1] Control 5.2: rollen en verantwoordelijkheden mbt informatiebeveiliging en privacy

Onderhoud en evaluatie

Dit beleid wordt minimaal jaarlijks geëvalueerd of bij significante wijzigingen in processen, systemen of wetgeving[2]. De Informatiebeveiligingcoördinator initieert wijzigingen en tussentijdse inhoudelijke updates van dit document. Alle wijzigingen worden ter evaluatie en effectuering aan de directie aangeboden. Het informatiebeveiligingsbeleid wordt besproken tijdens het directieoverleg en indien vastgesteld gedeeld via het intranet. Bij wijzigingen in het beleid worden deze via de afdelingshoofden kenbaar gecommuniceerd.

Nieuwe medewerkers ontvangen dit document bij indiensttreding, tezamen met het personeelshandboek en de inschrijving voor de eerste awareness cursus

Risicomanagement & Beveiligingsstrategie

We gebruiken op kantoor één cloudpakket voor planning en facturatie, maken gebruik van een gedeelde cloud-drive en hebben in de fabriek een machine.

Risico: uitval of gijzeling (ransomware) van cloudpakket & cloud-drive.
Kans: middel (veel aanvallen in de sector).
Impact: hoog (geen facturen, geen planning).
Bestaande maatregel: wachtwoord + back-up.
Conclusie: extra maatregel nodig → Multi Factor Authenticatie en test van back-upherstel.

Risico: uitval of gijzeling (ransomware) van een machine.
Kans: middel tot hoog (het is een ouder systeem)
Impact: hoog (geen productie)
Bestaande maatregel: geen
Conclusie: extra maatregel nodig -> contact met de leveranciers voor updates en ‘isolatie’ van het systeem.

Overige risico’s, zoals datalekken, worden in beginsel als geaccepteerd risico beschouwd, indien ze voorkomen worden passende acties genomen.

[2] Control 5.1 Beleid voor informatiebeveiliging, Formeel beleid, jaarlijks herzien

Maatregelen

Personeel en privacy

Aanname van personeel

Personeel wordt voordat er een contract wordt getekend gevraagd om een VOG.[3] Ook wordt er pas een contract ondertekend als er een kopie paspoort/rijbewijs of ID is overhandigd. Deze wordt veilig opgeslagen voor de duur van het contract.

Bewustwording en Training[4]

- We voeren een jaarlijkse security awareness-training uit voor medewerkers (verantwoordelijkheid HR)
- Praktische oefeningen en simulaties van phishingaanvallen (verantwoordelijkheid IT)
- Pentesten (verantwoordelijkheid IT)
- Beleid voor het melden van beveiligingsincidenten (verantwoordelijkheid IBC)
- Jaarlijkse review van dit document, inclusief heranalyse risicoprofiel onder begeleiding en met training van een externe consultant (directie)

Externen[5][6]

Er wordt voor gezorgd dat de in de opdracht genoemde persoonsgegevens en vertrouwelijke gegevens uitsluitend gebruikt worden voor de doeleinden in de opdracht. Dit staat zo in de opdracht vermeld. Incidenteel wordt hier een controle op uitgevoerd door IBC met hulp van IT. De verwerkersovereenkomsten worden bijgehouden in een register waarin vermeld staat doel van de verwerkersovereenkomst, ingangsdatum, einddatum en eventuele controle en opmerkingen.

Website

Informatie van de website wordt alleen gebruikt nadat een bezoeker middels cookies hiervoor toestemming heeft gegeven.

Fysieke Beveiliging[7]

Brasholt Hekwerk BV kent drie hoofdzones:

- **Fabrieksruimte (productieomgeving)**
  Bevat machines en apparatuur voor metaalbewerking en assemblage.
- **Kantooromgeving**
  Huisvest administratieve, plannings- en ondersteunende functies.
- **Directiekantoor**
  Aparte ruimte voor directie en vertrouwelijke vergaderingen.

---

[3] Control 6.1 achtergrond personeel
[4] Control 6.3 kennis personeel op peil brengen / houden
[5] Control B8.2.2 verwerkingsdoeleinden
[6] Control B8.26 registratie ter controle
[7] Control 7.1: Worden er fysieke beveiligingszones gehanteerd?

Toegang tot elke ruimte is **fysiek gescheiden** en uitsluitend mogelijk met **specifieke sleutels**.
Sleutels zijn **gepersonaliseerd uitgegeven**: alleen medewerkers met een geldige reden tot toegang tot een ruimte ontvangen de betreffende sleutel(s).
Een register van sleutels en sleutelhouders wordt bijgehouden door de **IBC**

Beveiligingsgedrag van medewerkers
Als een ruimte is ontgrendeld, zijn aanwezige medewerkers verantwoordelijk voor het toezicht op binnenkomst. Bij het betreden of verlaten van een ruimte wordt gecontroleerd of er geen onbevoegden meelopen (tailgating). Onbekende of ongeautoriseerde personen worden altijd aangesproken en begeleid naar de receptie of verantwoordelijke persoon.

Beheer van toegang
Bij verlies van een sleutel wordt dit onmiddellijk gemeld aan de directie en de IBC
Periodiek wordt geëvalueerd of de toegang nog aansluit bij de functie van de medewerker. Indien nodig wordt de sleutel ingenomen. De toegang van bezoekers of externe partijen (zoals onderhoudstechnici) wordt tijdelijk verleend onder toezicht.

Op deze manier hebben alleen geoorloofde personen toegang tot ook de systemen die in de zones aanwezig zijn.[8]

Digitale toegangsbeveiliging

Accountbeheer[9][10]

- Elke medewerker heeft een uniek account, waardoor acties altijd terug te voeren is naar een individu[11]. Het wachtwoord is minimaal 10 karakters lang en wordt jaarlijks gewijzigd. Elk account gebruikt multi-factor authenticatie.
- Brasholt Hekwerk gebruikt standaard **authenticator apps** (Microsoft Authenticator) of sms-code als tweede factor.
-
- Nieuwe accounts worden alleen aangemaakt op aanvraag van de leidinggevende van de medewerker.
- Wijzigingen in rollen of functies worden direct doorgegeven door de leidinggevende aan de IT-beheerder zodat toegangsrechten aangepast kunnen worden.
- Bij uitdiensttreding worden accounts direct geblokkeerd en binnen 24 uur verwijderd. HR manager geeft dit door aan de IT beheerder.

[8] Control 5.15: beleid voor toegangsbeveiliging
[9] Control 5.16: account beheer
[10] Control 5.18 toegangsrechten verlenen en beheersen
[11] Control 8.5: gebruikers controleren wie ze zijn

Authorisatiematrix[12][13][14]

Rol / Functie	E-mail	ERP (orders)	Financiële administratie	HR-dossiers	Productie-systeem	Beheerrechten
Directie	Lezen/ Schrijven	Lezen	Lezen/ Goedkeuren	Lezen	Geen toegang	Geen
Informatiebeveiligings-coördinator (IBC)	Lezen/ Schrijven	Geen	Geen	Geen	Geen toegang	Lezen/ Goedkeuren
Administratie	Lezen/ Schrijven	Lezen/ Schrijven	Lezen/ Schrijven	Geen	Geen toegang	Geen
HR	Lezen/ Schrijven	Geen	Geen	Lezen/ Schrijven	Geen toegang	Geen
Functionaris gegevensbescherming (FG)	Lezen/ Schrijven	Geen	Geen	Lezen	Geen toegang	Geen
Productiemedewerker	Lezen/ Schrijven	Geen	Geen	Geen	Lezen/ Schrijven	Geen
Teamleider Productie	Lezen/ Schrijven	Lezen	Geen	Geen	Lezen/ Schrijven	Geen
IT-beheer	Beheer-rechten	Beheer-rechten	Beheer-rechten	Beheer-rechten	Beheer-rechten	Volledig

Bij indiensttreding geeft HR aan IT aan wanneer de persoon in dienst komt. De afdelingsmanager geeft aan welke rollen een nieuwe medewerker – en dus welke bijbehorende permissies - hoort te krijgen. Dit wordt goedgekeurd door de directie.
De directie is ook in staat om IT beheer te controleren, net als de informatiebeveiligingscoordinator. Bij uitdiensttreding en/of bij einde contract van externen geeft HR een seintje aan IT, die ervoor zorg draagt dat bij de datum uitdiensttreding de rechten van de desbetreffende persoon worden ingetrokken. Jaarlijks gaat IBC beheer een controle uitvoeren op de systemen en ingestelde rechten.

Als er een – tijdelijke – uitzondering gemaakt moet worden, kan dit aangevraagd worden bij IBC die - na een controle met positief resultaat door de directie – dit ten uitvoer zal laten brengen door IT. Deze uitzonderingen worden hieronder bijgehouden en automatisch teruggetrokken indien niet meer nodig.

[12] Control 5.15: beleid voor toegangsbeveiliging
[13] Control 5.16: account beheer
[14] Control 5.18 toegangsrechten verlenen en beheersen

Lijst uitzonderingen:

Wie	id	Aanvullende permissies	Einde datum
Stagiair Bennie	bennie@brasholt.nl	HR lezen	31-12-2026
Externe consultant van leverancier tbv ERP	jitse@brasholt.nl	ERP lezen,schrijven & beheerrechten	31-07-2026

Controle en logging[15]

Er wordt logging bijgehouden van aanmeldingen, foutieve pogingen[16] en wijzigingen in rechten.
De IT-beheerder voert elk kwartaal een review uit van actieve accounts en toegangsrechten.
Logging wordt dusdanig opgeslagen dat deze alleen toegangelijk is voor IT en directie

Netwerk- en Systeembeveiliging[17]

Brasholt Hekwerk BV hanteert diverse technische maatregelen om de betrouwbaarheid, beschikbaarheid en integriteit van haar netwerken en systemen te waarborgen. De volgende componenten vormen de kern van het netwerk- en systeembeveiligingsbeleid:

Firewallbeheer
Alle inkomend en uitgaand verkeer verloopt via een centrale firewall. De werking en configuratie van deze firewall wordt maandelijks gecontroleerd door de IT-beheerder.

Antivirusbescherming[18]
Alle werkplekken, laptops en servers zijn voorzien van een centrale virusscanner met real-time detectie. IT controleert wekelijks of de virusdefinities up-to-date zijn en of er verdachte activiteiten zijn gedetecteerd. In geval van besmetting wordt het apparaat onmiddellijk geïsoleerd.

Netwerksegmentatie
Het bedrijfsnetwerk is opgedeeld in logische segmenten:

- Productieomgeving
- Kantooromgeving
- Gastennetwerk (Wi-Fi)

Deze segmentatie zorgt ervoor dat ongeautoriseerde toegang tussen zones wordt voorkomen.
Werkplekken zijn zo geconfigureerd dat alleen noodzakelijke verbindingen mogelijk zijn tussen afdelingen.

---

[15] Control 8.15 (2/2) logbestanden
[16] Control 8.20 (1/2) informatie op het netwerk beheren
[17] Control 8.20 (2/2) informatie op het netwerk beheren

[18] Control 8.7: bescherming tegen malware

VPN voor externe toegang[19]
Laptops die buiten kantoor worden gebruikt, verbinden via een beveiligde VPN-verbinding. IT beheer beheert de VPN-toegang en verleent deze alleen aan gebruikers met een functionele noodzaak (zoals directie, administratie en sales). Toegang is gekoppeld aan MFA.
In het personeelshandboek is opgenomen dat bij vertrouwelijke gesprekken de medewerker in een afgesloten ruimte moet zitten, zonder dat anderen kunnen meeluisteren.

Encryptie van apparaten[20]
Alle laptops en mobiele apparaten die bedrijfsgegevens kunnen bevatten, zijn verplicht voorzien van volledige schijfversleuteling (bijv. BitLocker of FileVault). IT beheer controleert jaarlijks of deze versleuteling actief is op de laptops van medewerkers
Gegevens op verloren of gestolen apparaten blijven daarmee onleesbaar voor onbevoegden.

Beveiligde draadloze netwerken
Alle Wi-Fi-netwerken binnen Brasholt Hekwerk zijn beveiligd met WPA2- of WPA3-encryptie. Gastgebruikers maken gebruik van een gescheiden netwerk zonder toegang tot interne systemen. Het wachtwoord van het interne netwerk wordt periodiek gewijzigd.

Software-updates en andere veranderingen [21]
Automatische updates zijn ingeschakeld voor alle besturingssystemen[22], antivirussoftware en kritieke applicaties op werkstations en servers. IT controleert via centraal beheer of updates succesvol zijn toegepast en grijpt in bij storingen.

Voor grote veranderingen, updates of nieuwe installaties wordt dit eerst in een test omgeving uitgevoerd, dus voordat er productie wordt gedraaid. Pa als er geen incidenten zijn waarvan de directie vindt dat die onacceptabel zijn, gaat de update (of nieuwe installatie) 'live'. Dit is verantwoordelijkheid van de IT beheerder met een approval van de directie om de restpunten te accepteren.

Schermvergrendeling en time-out
Werkstations en laptops zijn zo ingesteld dat het scherm automatisch vergrendelt na maximaal 10 minuten inactiviteit. IT ziet toe op correcte instellingen via groepsbeleid of device management.

[19] Control 6.7 informatie via remote access (telewerken)
[20] Control 8.24: versleuteling
[21] Control 8.32: beheerst uitvoeren veranderingen
[22] Control 8.8: voorkomen exploitatie van kwetsbaarheden

Leveranciersbeheer & Softwareontwikkeling[23][24]

Brasholt Hekwerk BV ontwikkelt geen eigen software. [25]
Brasholt Hekwerk BV werkt met externe leveranciers als onderdeel van onze ICT-diensten en systeembeheer en leveren van onze machines. Om risico's op het gebied van informatiebeveiliging te beheersen, is het essentieel dat ook leveranciers voldoen aan passende beveiligingsmaatregelen.

Beoordeling van leveranciers

- Voorafgaand aan samenwerking met een nieuwe leverancier wordt een leveranciersbeoordeling uitgevoerd, waarin onder andere wordt gekeken naar:
  Het beveiligingsniveau van de leverancier (ISO 27001-certificering of vergelijkbare gecertificeerde maatregelen).
- De omgang met updates, patches en incidentmanagement.

De beoordeling wordt uitgevoerd door de Informatiebeveiligingscoördinator in samenwerking met de directie.

Contractuele afspraken[26]
In alle contracten met leveranciers wordt standaard opgenomen:

- Welke beveiligingsmaatregelen minimaal worden verwacht (zoals encryptie, toegangscontrole, logging, meldingen van incidenten en recht van audits))
- Verplichtingen rondom meldingen van beveiligingsincidenten
- Geheimhoudingsclausules (NDA)
- Eigendom van data en bewaartermijnen

Bestaande leveranciers worden minimaal jaarlijks geëvalueerd, of eerder bij incidenten of wijzigingen in dienstverlening. Indien een leverancier niet (meer) aan de eisen voldoet, worden beheersmaatregelen getroffen of wordt de samenwerking beëindigd.

Continuïteitsbeheer & Herstelmaatregelen

Dagelijkse back-ups worden automatisch gemaakt van alle bedrijfskritische systemen, inclusief het ERP-systeem, klantendatabase en administratieve bestanden.2
Back-ups worden zowel lokaal (NAS-systeem op kantoor) als in een beveiligde cloudomgeving opgeslagen, volgens het 3-2-1-principe:
3 kopieën van de data
2 verschillende media
1 offsite back-up

IT is verantwoordelijk voor het beheer, toezicht en controle van het back-up proces.

---

[23] Control 5.22 Dienstverlening van leveranciers managen
[24] Control 8.26 informatiebeveiliging in aanschaf van (nieuwe) applicaties
[25] Control 8.25 security by design bij software ontwikkeling (niet-toepasbaar: NVT).
[26] Control 8.21 veiligheid van netwerkdiensten

Disaster Recovery Plan (DRP)

Brasholt Hekwerk heeft een Disaster Recovery Plan (DRP) opgesteld voor de meest kritieke systemen, als bijlage van dit document.
Hierin staat beschreven:

- Welke systemen prioritair hersteld moeten worden
- Welke stappen gevolgd moeten worden bij uitval of rampen (brand, ransomware, stroomuitval)
- Wie welke verantwoordelijkheden heeft binnen het herstelproces
- Waar de back-ups zich bevinden en hoe deze toegankelijk zijn

Het DRP is bewaard in zowel fysieke als digitale vorm en wordt jaarlijks geëvalueerd en is dusdanig opgesteld dat ook tijdens calamiteiten de informatie beschikbaar, integer en vertrouwelijk wordt behandelt.[27]

Testen van herstelprocedures

Minimaal een keer per jaar wordt er een testherstel uitgevoerd op een representatief systeem om te controleren of back-ups volledig en correct teruggezet kunnen worden.
De resultaten van de test worden door IT gedocumenteerd en besproken met de directie.
Bevindingen leiden, indien nodig, tot aanpassingen in het back-upbeleid of DRP.

Beleid voor het melden van beveiligingsincidenten

Een beveiligingsincident is elke gebeurtenis die de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of systemen in gevaar brengt. Voorkomende zijn bijvoorbeeld:

- Phishing-aanvallen (aanvallen via e-mail, telefoon, whatsapp of sms)
- Ransomware/malware-infecties (= urgent!)
- Ongeautoriseerde toegang tot systemen
- Dataverlies of datalekken
- Ongebruikelijke netwerkactiviteit
- Een kwetsbaarheid die zichtbaar wordt
- E-mail per ongeluk aan verkeerde afzenders gestuurd.

Wie moet melden?[28]

Alle medewerkers, leveranciers en externe partijen die toegang hebben tot de systemen of gegevens van het bedrijf zijn verplicht om beveiligingsincidenten direct te melden.
Medewerkers zijn op de hoogte via dit beleid, externen worden geinformeerd via een verwerkersovereenkomst danwel inkoop/verkoopcontracten.

[27] Control 5.29 (1/2) informatiebeheer tijdens calamiteiten
[28] Control 6.8: rapportage van informatiebeveiligingsgebeurtenissen

Hoe een incident te melden?

Een beveiligingsincident moet onmiddellijk worden gemeld via de volgende kanalen:
E-mail intern: 911@Brasholt Hekwerk.nl
indien urgent onmiddellijk gevolgd door:
Telefoon: 911

Bij melding moet zoveel mogelijk de volgende informatie worden verstrekt:

- Datum en tijdstip van het incident;
- Beschrijving van wat er is gebeurd;
- Betrokken systemen of accounts;
- Eventuele verdachte e-mails, bijlagen of links;
- Acties die al zijn ondernomen (alleen indien van toepassing).

Acties bij een incident

In eerste instantie organiseert de IBC de afhandeling van het incident. Afhankelijk van het type incident kunnen de volgende stappen worden genomen:
Phishing → Waarschuwen personeel en blokkeren verdachte afzenders.
Malware-infectie → Isoleren van het getroffen systeem en scannen op malware (via IT)
Datadiefstal → Logbestanden[29] analyseren, mogelijk datalek melden bij de Autoriteit Persoonsgegevens (AVG).
Ongeautoriseerde toegang → Direct wachtwoord reset en extra monitoring.

Indien een incident bedrijfsprocessen verstoort of persoonsgegevens betreft, wordt het voor het extern melden (bv bij AP), geëscaleerd naar:

1. Directie;
2. Waarna externe IT-beheerder / externe IT-partner / toeleverancier / klanten geïnformeerd worden
3. Externe instanties (bij ernstige datalekken, conform AVG bij AP en RDI voor CBW).

In geval van een crisis wordt een crisisteam geformeerd waarbij de directeur, externe consultant cybersecurity , IT, woordvoering en IBC deelneemt. Alle overige personeelsleden staan standby. Er wordt gewerkt met de BOB structuur (Beeldvorming-oordeelsvorming-besluitvorming). Alle betrokkenen hebben – eventueel met een verwerkersovereenkomst – de verplichting de informatie beschikbaar, integer en vertrouwelijk te behandelen. [30]

[29] Control 8.15 (1/2) logbestanden
[30] Control 5.29 (2/2) informatiebeheer tijdens calamiteiten

Registratie van een incident

Elk incident wordt gelogd ten behoeve van periodieke rapportages en jaarlijkse her-ijking van het risicoprofiel. Het register is toegevoegd als .xls toegevoegd als bijlage aan dit document. Het bevat een omschrijving van het incident, datum, actiehouder en vervolgstap.

Compliance & Audit

Dit informatiebeheersbeveiligingsbeleidsdocument wordt jaarlijks intern ge-evalueerd als onderdeel van onze audit.
We hebben een externe auditor voor het verkrijgen van het CYRA-IT, level3 certificaat. Onze IBC is verantwoordelijk voor de rapportage, certificering en de consequenties en te nemen maatregelen bij niet-naleving (door escalatie naar de directie).

Referenties / bijlagen

- Meldingsformulier incidenten
- Leveranciersbeoordeling format
- Verwerkersovereenkomstregister
- inkoop/verkoop overeenkomsten voor clausules mbt melden en toeleveranciers
- register van uitgave sleutels met toegang tot fysieke ruimtes
- Disaster Recovery Plan
- Incidentenregister