

1. Inleiding

Veel medewerkers van Ballast Nedam maken in diverse vormen gebruik van computerfaciliteiten. Daarnaast zijn er gebruikers van deze computerfaciliteiten die geen Ballast Nedam medewerker zijn. Het is van belang dat zorgvuldigheid wordt betracht bij dit gebruik, door welke gebruiker dan ook. Aan computerfaciliteiten, waaronder internet en e-mail, zijn grote voordelen, maar ook risico's verbonden. Daarom worden in deze gedragscode regels en voorwaarden gesteld aan het gebruik van computerfaciliteiten. Bij het opstellen en toepassen van deze gedragscode wordt gestreefd naar een goede balans tussen controle op verantwoord gebruik van de computerfaciliteiten en de bescherming van de privacy van de werknemers op de werkplek.

Doelstelling

Het instellen van deze gedragscode heeft tot doel de regels en voorwaarden voor het gebruik van computerfaciliteiten, inclusief de wederzijdse rechten en plichten van de werkgever en de werknemer, bekend te maken. Daarnaast wordt beoogd te voorkomen dat:

- Misbruik en overbelasting van de computerfaciliteiten ontstaan;
- Onnodige vergissingen, incidenten of schade door het gebruik van de computerfaciliteiten optreden;
- Schade aan de goede naam van Ballast Nedam wordt aangebracht.

Gehanteerde begrippen

In deze gedragscode worden de volgende begrippen gehanteerd:

- Beheerder: degene die toezicht houdt op het functioneren van de computerfaciliteiten van Ballast Nedam. Binnen Ballast Nedam wordt deze functie ingevuld door Ballast Nedam ICT (BNICT), met als aanspreekpunt de BNICT Helpdesk (helpdesk@ballast-nedam.nl / +31 30 2853500);
- Computerfaciliteiten: alle (ICT) hulpmiddelen die worden gebruikt voor de geautomatiseerde informatievoorziening, waaronder apparatuur, programmatuur, netwerken, internet en e-mail;
- Gebruiker: degene die gebruik maakt van de computerfaciliteiten van Ballast Nedam;
- Security Manager ICT (SMI): aanspreekpunt binnen BNICT voor alle zaken op het gebied van informatiebeveiliging, die gerelateerd zijn aan ICT-systemen, technische infrastructuur en applicaties;
- Spam: onpersoonlijke, ongevraagde commerciële emailberichten of ongevraagde massale emailberichten;
- Phishing: ongewenste emailberichten met als doel het verkrijgen van persoonlijke gegevens zoals inlognamen, wachtwoorden etc. teneinde ongeautoriseerde toegang te krijgen tot ICT-systemen;
- Werkplek: de plaats waar het gebruik van de computerfaciliteiten plaatsvindt, inclusief de apparatuur die hiervan onderdeel uitmaakt.

Werkingsfeer

Deze gedragscode is van toepassing op:

- Eenieder die in het kader van zijn werk gebruik maakt van computerfaciliteiten die eigendom zijn van, en ter beschikking gesteld worden door Ballast Nedam;
- Gevallen waarin Ballast Nedam haar computerfaciliteiten beschikbaar stelt aan derden: deze worden op de hoogte gebracht van de gedragsregels. De gedragsregels zijn ook op hen van toepassing;
- Overige personen aan wie het recht tot het gebruik van de computerfaciliteiten van Ballast Nedam is verleend.

2. Algemene regels en voorwaarden

- 2.1. De aan de gebruiker ter beschikking gestelde computerfaciliteiten zijn bedoeld voor zakelijk gebruik. Privé-gebruik wordt alleen toegestaan als dit de dagelijkse werkzaamheden niet negatief beïnvloedt en niet schadelijk is voor de (prestaties van) computerfaciliteiten van Ballast Nedam.
- 2.2. Het is niet toegestaan computerfaciliteiten van Ballast Nedam te gebruiken of te exploiteren voor commerciële doeleinden anders dan die welke voortvloeien uit hoofde van de functieervulling bij Ballast Nedam, tenzij hiervoor expliciet toestemming van de leidinggevende is verkregen.
- 2.3. De gebruiker is verplicht zich te houden aan algemene instructies voor het gebruik van computerfaciliteiten. Instructies en aanwijzingen die tijdens het gebruik van computerfaciliteiten worden gegeven moeten worden opgevolgd.
- 2.4. Toegang tot computerfaciliteiten van Ballast Nedam wordt verleend op basis van een combinatie van gebruikersnaam en een persoonlijk wachtwoord of andere vergelijkbare identificatie- en authenticatiemiddelen.
- 2.5. Voor het beheer van het persoonlijke wachtwoord gelden de volgende regels:
 - De gebruiker is verantwoordelijk voor het gebruik van de bevoegdheden die aan de combinatie van gebruikersnaam en wachtwoord zijn verbonden. De gebruiker moet dus alle redelijke maatregelen voor de beveiliging en geheimhouding van het wachtwoord hebben getroffen;
 - Het wachtwoord is strikt persoonlijk en niet overdraagbaar;
 - Ten aanzien van het wachtwoord is geheimhouding verplicht;
 - De gebruiker zal bij constatering van misbruik van zijn combinatie van gebruikersnaam en wachtwoord BNICHT hierover direct informeren.
- 2.6. De gebruiker zal zijn werkplek zorgvuldig gebruiken en beheren en ervoor zorgdragen dat deze werkplek bij tijdelijke of langdurige afwezigheid niet onbeheerd wordt achtergelaten. Een screensaver met wachtwoordmechanisme moet worden gebruikt bij kortdurende afwezigheid.
- 2.7. De gebruiker is verantwoordelijk voor het actief zijn van een actueel anti-virusprogramma op de PC/Laptop waarmee een verbinding wordt gemaakt met de ICT Infrastructuur, ook als deze niet door Ballast Nedam ter beschikking is gesteld. Vereist is dat dit programma periodiek, in ieder geval dagelijks, wordt geactualiseerd;
- 2.8. Incidenten die het normale gebruik van de voorzieningen verstoren dienen direct bij BNICHT gemeld te worden. Hieronder vallen ook beveiligingsincidenten waar de gebruiker weet van heeft, maar niet zelf onmiddellijk hinder van heeft.
- 2.9. Het is niet toegestaan om zelf vaste apparatuur te verhuizen, verplaatsen en/of te ruilen en/of netwerkaansluitingen te wijzigen zonder voorafgaand overleg met BNICHT. Gewenste verhuizingen, verplaatsingen en/of ruilingen kunt u aanvragen bij BNICHT.
- 2.10. De gebruiker draagt zelf de verantwoordelijkheid de vereiste kennis op te doen om met de apparatuur en programmatuur te kunnen werken. Hij of zij kan - na goedkeuring van de direct leidinggevende - een cursus volgen.
- 2.11. Het is de gebruiker niet toegestaan zich ongeautoriseerd toegang te verschaffen tot gegevens van andere gebruikers of ongeautoriseerd programma's te gebruiken.
- 2.12. Het is de gebruiker niet toegestaan de door Ballast Nedam ter beschikking gestelde programmatuur, gegevensbestanden of documentatie ongeautoriseerd te kopiëren of ter beschikking te stellen aan derden.
- 2.13. De gebruiker zal geen acties ondernemen of pogingen hiertoe doen die de continuïteit of de beveiliging van de computerfaciliteiten van Ballast Nedam ondermijnen.
- 2.14. Het is niet toegestaan andere gebruikers met behulp van de computerfaciliteiten onheus te bejegenen of lastig te vallen.
- 2.15. De gebruiker zal zorgvuldigheid betrachten bij het gebruik en het beheer van mobiele apparatuur en gegevensdragers. Dit geldt ook voor het aansluiten van mobiele apparatuur op het netwerk van Ballast Nedam.

- 2.16. De gebruiker is verantwoordelijk voor het afdrukken van gegevens op printers en zal de vertrouwelijkheid van afgedrukt materiaal waarborgen.
- 2.17. Het is niet toegestaan applicaties te (laten) installeren zonder toestemming van BNIC. Het is niet toegestaan applicaties te (laten) installeren waarvoor Ballast Nedam geen licentie(s) bezit. Gebruikers dienen zich te houden aan de bepalingen in de licentieovereenkomst(en).

3. Regels en voorwaarden voor het gebruik van e-mail en internet

- 3.1. Het gebruik van het aan de gebruiker op persoonlijke titel ter beschikking gestelde emailadres is strikt persoonlijk. Niet persoonsgebonden emailadressen kunnen wel met meerdere gebruikers worden gedeeld, waarbij altijd één gebruiker als aanspreekpunt voor het emailadres wordt aangesteld.
- 3.2. Het is de gebruiker niet toegestaan om:
 - o Een niet voor hem geldend emailadres te gebruiken;
 - o Emailberichten op enigerlei wijze te vervalsen;
 - o Met behulp van de computerfaciliteiten van Ballast Nedam spam te versturen;
 - o Voor andere gebruikers bestemde emailberichten doelbewust ongeautoriseerd te lezen, kopiëren, wijzigen, door te sturen of te vernietigen.
- 3.3. Het is niet toegestaan informatie die strijdig is met de wet of de goede zeden (o.a. pornografisch materiaal), informatie die de goede naam van Ballast Nedam aantast, informatie die een discriminerend, opruiend, aanstootgevend of bedreigend karakter heeft met behulp van computerfaciliteiten van Ballast Nedam te produceren, benaderen, op te slaan, te verzenden of in de openbaarheid te brengen.
- 3.4. Het is gebruikers niet toegestaan elektronische kettingsbrieven of waarschuwingsberichten van virussen aan (groepen van) gebruikers te verzenden.
- 3.5. Het is niet toegestaan auteursrechtelijk beschermd materiaal, waaronder programmatuur, teksten, beeldmateriaal of muziek, te kopiëren, te downloaden of aan derden ter beschikking te stellen zonder toestemming van de auteursrechthebbende. Bovendien moet bij het downloaden alles in het werk worden gesteld om het binnenhalen van virussen te voorkomen en de beschikbaarheid van de computerfaciliteiten niet in gevaar te brengen.
- 3.6. Het is niet toegestaan vertrouwelijke informatie, op internet onbeveiligd ter beschikking te stellen of onbeveiligd via openbare netwerken (o.a. e-mail via internet) te verspreiden.
- 3.7. Elke gebruiker heeft een persoonlijke toegang tot computerfaciliteiten en de bijbehorende systeemauthorisaties gekregen. De gebruiker mag deze toegang niet door anderen laten gebruiken.
- 3.8. De gebruiker zal al wat redelijkerwijs van hem/haar mag worden verlangd, doen om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens die aanwezig zijn op de voor hem/haar toegankelijke informatiesystemen te waarborgen.
- 3.9. De gebruiker is verplicht alle redelijke voorzorgsmaatregelen te treffen ter voorkoming van diefstal van apparatuur en/of media.
- 3.10. Een gebruiker mag zich op het internet niet ongeoorloofd toegang verschaffen tot niet-openbare bronnen of toegangsrechten van gebruikers van Ballast Nedam te misbruiken en hierdoor deze bronnen aan derden ter beschikking stellen.
- 3.11. Bij deelname aan discussiegroepen en sociale netwerken, of andere platforms, op het internet mag een gebruiker geen mededelingen doen namens Ballast Nedam, maar moet aangegeven worden dat meningen op persoonlijke titel worden geuit. Medewerkers die Ballast Nedam of één van haar bedrijfsonderdelen vertegenwoordigd op social media spreken namens het bedrijf in het openbaar en dienen daarom een aantal richtlijnen in ogenschouw te nemen zoals deze zijn opgesteld door de afdeling Communicatie.
- 3.12. Wanneer de beveiliging of de continuïteit van de elektronische berichtenvoorziening dit vereist, is de beheerder gerechtigd voor gebruikers bestemde berichten te lezen, kopiëren, te vernietigen of bijlagen te verwijderen.

- 3.13. Wanneer een email account van een gebruiker vanwege langdurige afwezigheid, bijvoorbeeld door ziekte, niet gebruikt kan worden kan dit email account aan de direct leidinggevende worden toegewezen teneinde de bedrijfsvoering niet in gevaar te brengen.
- 3.14. Bij uitdienststreding van een medewerker zal zijn email account worden overgedragen aan zijn leidinggevende.
- 3.15. Eventuele persoonlijke emailberichten dienen in een aparte map te worden opgeslagen.

4. Externe toegang

- 4.1. De gebruiker zal bij de uitoefening van zijn werkzaamheden waarbij externe toegang tot informatiesystemen gebruikt wordt, de grootst mogelijke zorgvuldigheid in acht nemen.
- 4.2. De gebruiker neemt maatregelen om te voorkomen dat derden informatie te zien krijgen, die niet voor hen bestemd is. Er wordt vanuit gegaan dat minimaal de volgende maatregelen genomen zijn om dit te bereiken:
 - o Apparatuur mag niet onbeheerd achtergelaten worden, ook niet voor korte tijd;
 - o Bij langdurige inactiviteit of afwezigheid moet de apparatuur worden uitgezet;
 - o Derden mogen niet mee (kunnen) lezen.

5. Informatiebeveiliging

- 5.1. Na het geven van een printopdracht moet een gebruiker de afgedrukte pagina's direct uit de printer halen. Dit ter voorkoming dat andere mensen de output lezen en/of meenemen.
- 5.2. Bedrijfsgegevens en gegevensdragers moeten vertrouwelijk en zorgvuldig worden behandeld en bewaard, elke gebruiker is hiervoor zelf verantwoordelijk. De databestanden moeten worden bewaard in de juiste (sub)directories of mappenstructuur.
- 5.3. Voor het gebruik van gegevensdragers moet men apparatuur benutten welke beveiligd is, en bij voorkeur door Ballast Nedam ter beschikking is gesteld.
- 5.4. Gegevensdragers die buiten Ballast Nedam zijn gebruikt moeten virusvrij zijn. Een gebruiker kan verantwoordelijk worden gesteld voor de schade die ontstaat als apparatuur en/of programmatuur wordt besmet met een virus vanwege onkundig handelen.

6. Aanmelden van storingen, problemen en/of wensen

- 6.1. Bij problemen met apparatuur en programmatuur die door de organisatie ter beschikking is gesteld, moet contact worden opgenomen met de BNICT Helpdesk op nummer [+31 30 285 3500]. Via email is de BNICT Helpdesk te bereiken onder het mailadres: helpdesk@ballast-nedam.nl.
- 6.2. De BNICT Helpdesk is op werkdagen van 7:00 tot 17:00 uur bereikbaar.
- 6.3. Voor het correct aannemen van de wens en/of storing heeft de medewerker van BNICT in ieder geval de onderstaande gegevens nodig:
 - o Naam;
 - o Afdeling;
 - o Telefoonnummer;
 - o Het assetnummer van de PC;
 - o Een duidelijke probleemomschrijving.
- 6.4. De aangemelde wens en/of storing wordt geregistreerd in een geautomatiseerd administratie- / bewakingssysteem en zo mogelijk direct telefonisch verholpen. Hiervoor beschikt de medewerker van BNICT over een programma waarmee het mogelijk is om uw apparatuur, toetsenbord en muis na verkregen toestemming over te nemen vanaf zijn eigen werkplek.

7. Privacy, toezicht en controle

- 7.1 De verantwoordelijkheid voor en het toezicht op het juiste gebruik van de computerfaciliteiten van Ballast Nedam ligt bij de direct leidinggevende van de gebruiker(s).

- 7.2 Controle op het gebruik van computerfaciliteiten, waaronder e-mail en internet, vindt alleen plaats in het kader van de doelstelling van deze gedragscode en het beheer van de computerfaciliteiten.
- 7.3 In het kader van technisch systeem- en netwerkbeheer vindt vastlegging van gebruikers- en verkeerinformatie (logging) plaats. Deze gegevens worden niet langer dan een periode van zes maanden bewaard.
- 7.4 De Security Manager ICT heeft het recht om namens de Raad van Bestuur na een gerezen verdenking van handelen in strijd met deze gedragscode, in het kader van een onderzoek voor een beperkte periode gerichte controle uit te laten voeren door de beheerder op e-mail-, netwerkverkeer of internetgebruik van individuele gebruikers. De directie of een namens de directie daartoe aangewezen functionaris van het betreffende bedrijfs onderdeel moet vooraf toestemming geven voor het uitvoeren van deze gerichte controle.
- 7.5 Bij geconstateerde (beveiligings)incidenten heeft de beheerder het recht om apparatuur en/of gebruikers de toegang tot computers en/of netwerken (tijdelijk) te ontfeggen.
- 7.6 Leden van de Raad van Bestuur, ondernemingsraad en andere medewerkers met een specifieke vertrouwensfunctie die daartoe door de Raad van Bestuur zijn aangewezen, zijn gedurende hun wettelijke beschermingsperiode in beginsel uitgesloten van persoonlijke controle. Uitzonderingen hierop kunnen alleen worden gevormd door dat wat er in artikel 7.7 wordt gesteld.
- 7.7 Indien hiertoe gedwongen of gesommeerd door een daartoe strekkende rechterlijke uitspraak, zal de Raad van Bestuur medewerking verlenen aan verstrekking van informatie aangaande gebruik van computerfaciliteiten door individuele gebruikers.
- 7.8 Gebruikers hebben met betrekking tot dat wat er over hen in het kader van het gebruik van computerfaciliteiten is vastgelegd de volgende rechten: inzagerecht, recht op correctie, recht op kopiëren, recht op verwijdering en vernietiging wanneer vastlegging van deze gegevens niet meer ter zake doende is, en voor zover dit technisch mogelijk is.

8. Melding en sancties

- 8.1 Bij constatering van misbruik van computerfaciliteiten of gebruik in strijd met de gedragscode computerfaciliteiten, regelgeving of wettelijke bepalingen:
- o Moet daarvan melding worden gemaakt bij de ICT Helpdesk via nummer [+31 30 285 3500] of via de chatoptie op het Ballast Nedam intranet;
 - o Kan een sanctie worden opgelegd.
- 8.2 Ook iedereen die een (mogelijk) beveiligings- of datalek ontdekt, dient dat incident onmiddellijk te melden via bovengenoemde route.
- 8.3 Tegen het instellen van de sancties of andere acties op grond van deze gedragscode kan de gebruiker bezwaar maken volgens de klachtenregeling van Ballast Nedam.
- 8.4 Als er sprake is van een misdrijf, of overtreding zal aangifte worden gedaan bij de politie.

9. Overige bepalingen

- 9.1 Vaststelling van deze gedragscode geschiedt door de Raad van Bestuur volgens de gangbare besluitvormingsprocedure.
- 9.2 De Raad van Bestuur informeert de gebruikers voorafgaande aan de invoering en bij wijziging van deze gedragscode over de inhoud van deze code, waaronder hetgeen over toezicht en controle is opgenomen.
- 9.3 Evaluatie en eventuele wijziging van de inhoud en de werking van deze gedragscode vindt plaats na drie jaar en/of in geval van ingrijpende wijzigingen binnen de organisatie en/of het gebruik van computerfaciliteiten.
- 9.4 In alle gevallen waarin deze gedragscode niet voorziet, beslist de Raad van Bestuur.