Gebruiksreglement ICT-middelen en -voorzieningen van de Universiteit Utrecht

Art. 1 Begripsbepalingen.

In dit gebruiksreglement wordt verstaan onder:

a. ICT-middelen en -voorzieningen:
   De door of namens de Universiteit Utrecht (hierna: UU) ter beschikking gestelde hardware, software en netwerkfaciliteiten, evenals de door of namens de UU aangeboden voorzieningen t.b.v. elektronisch data- en spraakverkeer;

b. Beheerder:
   De afdeling van de UU verantwoordelijk voor de operationele beschikbaarheid van de ICT-middelen en -voorzieningen;

c. Gebruiker:
   Iedereen die als werknemer van de UU, student aan de UU of op andere basis rechtmatig toegang heeft verkregen tot de ICT-middelen en -voorzieningen;

Art. 2 Toegestaan gebruik

Het is gebruikers slechts toegestaan de ICT-middelen en -voorzieningen te gebruiken voor het uitvoeren van de functie of het volgen van onderwijs. Gebruik voor privé doeleinden is slechts toegestaan voor zover dit niet storend is voor de dagelijkse werkzaamheden van de desbetreffende gebruiker of van anderen.

Art. 3 Niet toegestaan gebruik

1. Verboden is elke vorm van gebruik van de ICT-middelen en -voorzieningen die inbreuk maakt op wet- en regelgeving of op de bepalingen van dit gebruiksreglement, die beheer, onderhoud, beveiliging, integriteit, kwaliteit en continuïteit van de door de UU aan haar gebruikers aangeboden dienstverlening in gevaar brengt, die de bedrijfsprocessen van de UU verstoort, of die de UU, gebruikers en/of derden financiële of imagoschade toebrengt.
2. Verder is het niet toegestaan:
   a) zelf aanvullende hardware en software op de ICT-middelen en -voorzieningen te installeren en/of op te starten, tenzij dit noodzakelijk is voor het uitvoeren van de functie of het volgen van onderwijs en dit past binnen de afspraken die met de beheerder van de betreffende ICT-middelen en –voorzieningen zijn gemaakt.
   b) met andermans naam gebruik te maken van de ICT-middelen en -voorzieningen en/of beveiligingsmaatregelen uit te schakelen of te omzeilen, dan wel de persoonlijke inlogcodes aan anderen bekend te maken;
   c) zich door middel van de ICT-middelen en -voorzieningen ongeoorloofd toegang te verschaffen tot niet-openbare en/of beveiligde informatiebronnen, dan wel anderen informatie te verschaffen uit dergelijke informatiebronnen;
   d) door middel van de ICT-middelen en –voorzieningen, die binnen de universitaire ruimten en terreinen beschikbaar worden gesteld, informatiebronnen te raadplegen die pornografisch, racistisch, discriminerend of aanstootgevend materiaal aanbieden, tenzij dit aantoonbaar noodzakelijk is voor het onderzoek of onderwijs van de gebruiker;
   e) informatie, waartoe men door middel van de ICT-middelen en -voorzieningen toegang heeft verkregen, ongeoorloofd te wijzigen, vernietigen of aan te vullen;
   f) de ICT-middelen en -voorzieningen zodanig te gebruiken, dat sprake is van overlast voor andere gebruikers en/of voor derden;
   g) de ICT-middelen en -voorzieningen in te zetten voor privé doeleinden met een commercieel karakter;
   h) de ICT-middelen en -voorzieningen te gebruiken voor het (door-)sturen van dreigende, beledigende, seksueel getinte, racistische of discriminerende berichten;
   i) met behulp van de ICT-middelen en -voorzieningen zonder toestemming van de rechthebbende auteursrechtelijk beschermde werken verspreiden. Het is slechts toegestaan software, films, muziek e.d. te downloaden, indien dit noodzakelijk is voor het uitvoeren van de functie of het volgen van onderwijs, met inachtneming van het auteursrecht en de door de UU afgesloten licentiecontracten.

Art. 4. Meldpunt

De UU heeft een meldpunt ingesteld, waar gebruikers melding kunnen maken van door hen geconstateerd niet toegestaan gebruik. Het hiervoor ingestelde emailadres is: abuse@uu.nl . Meldingen zullen vertrouwelijk worden behandeld; anonieme meldingen worden echter niet in behandeling genomen.

Art. 5. Registratie en controle

De UU duldt geen vormen van niet-toegestaan gebruik van de door haar ter beschikking gestelde ICT-middelen en -voorzieningen. Ter borging hiervan is een systeem van registratie en controle van het gebruik van de ICT-middelen en -voorzieningen in het leven geroepen. Dit houdt in, dat het gebruik wordt vastgelegd en dat op gezette tijden steekproefsgewijs een onderzoek naar dit gebruik plaatsvindt. Een onderzoek kan ook plaatsvinden als de UU hiervoor redenen aanwezig acht. Het onderzoek wordt uitgevoerd door de specifiek hiertoe aangewezen medewerker(s), of geschiedt langs geautomatiseerde weg. De bepalingen van de Wet Bescherming Persoonsgegevens zijn op de registratie van toepassing. De UU kan op grond van wettelijke bepalingen worden verplicht (deel-)gegevens uit deze registratie aan derden te verstrekken.

Art. 6. Sancties

Bij geconstateerde vormen van niet toegestaan gebruik zal de UU maatregelen jegens de overtreder(s) nemen. Bij het vaststellen van de vorm en de hoogte van de op te leggen sanctie zal o.a. rekening worden gehouden met de ernst van de bewuste overtreding(en), de tijdspanne waarop en de frequentie waarin de overtreding(en) voorkwamen, de gevolgen van de overtreding(en) en de hoogte van de eventuele ontstane materiële en immateriële schade. Voor zover het werknemers van de UU betreft, geldt voor het opleggen van sancties de universitaire regeling Orde- en disciplinaire maatregelen, die gebaseerd is op de CAO Nederlandse Universiteiten. Indien de UU dit wenselijk of noodzakelijk acht, kan zij overgaan tot het inschakelen van opsporingsinstanties. De UU kan daarnaast besluiten een privaatrechtelijke (schadevergoeding-)actie te starten.

Art. 7 Inwerkingtreding

Dit reglement treedt in werking op 1 maart 2008. Alle voorgaande reglementen op dit gebied zijn met de inwerkingtreding van dit gebruiksreglement vervallen.

Toelichting

Algemeen

Binnen de UU wordt op grote schaal gebruikt gemaakt van ICT-middelen en -voorzieningen. Nagenoeg alle bedrijfsprocessen zijn hier van afhankelijk. Om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en de informatievoorziening te beschermen, heeft het college van bestuur het universitair informatie beveiligingsbeleid vastgesteld. Dit beleid is vastgelegd in het document “Informatiebeveiliging Beleid en Basisregels Universiteit Utrecht”. Het doel van dit beleid is het inrichten en bewaken van een evenwichtig stelsel van beveiligingsmaatregelen, gericht op risicobeheersing. Door een samenstel van technische maatregelen en procedures wordt uitvoering gegeven aan het informatie beveiligingsbeleid.

Technische maatregelen alleen zijn niet voldoende om de goede werking van de ICT-middelen en voorzieningen te waarborgen. Ongewenst gebruik van de voorzieningen door een enkele gebruiker kan grote hinder en schade opleveren, waardoor andere gebruikers gedupeerd worden. Om dit te voorkomen zijn er regels opgesteld voor het verantwoord gebruik van de door de Universiteit Utrecht ter beschikking gestelde ICT-middelen. Deze zijn opgenomen in dit gebruiksreglement. Ieder die gebruik maakt van deze middelen dient zich daarbij te houden aan deze regels. Bij ICT-middelen kan gedacht worden aan gebruik van applicaties (waaronder e-mail en Internet), de computers, telefonie en het netwerk van de universiteit.

Dit reglement is in de eerste plaats van toepassing op de werknemers en de studenten van de Universiteit Utrecht die gebruik maken van de ICT-middelen binnen de gebouwen en op de terreinen van de universiteit. Daarnaast is het ook van toepassing bij gebruik van deze middelen van de universiteit (zoals het e-mailadres en de e-mailbox) buiten de universiteit. Voorts is het reglement van toepassing op alle andere personen die gebruik maken van de ICT-middelen van de Universiteit Utrecht, waaronder gedetacheerden, personen met een gastvrijheidovereenkomst, stagiaires, uitzendkrachten etc.

De kern van de regeling is weergegeven in artikel 2 en 3, waarin een aantal algemene regels is geformuleerd ten aanzien van respectievelijk het toegestaan en het niet toegestaan gebruik van de ICT-middelen. Met deze gebruiksregels streeft de Universiteit Utrecht naar het voorkomen van hinder of strafbare feiten door gebruik van voornoemde faciliteiten.
Er is voorzien in een meldpunt waar niet toegestaan gebruik gemeld kan worden. Daarnaast is er een systeem van registratie en controle. Bij niet toegestaan gebruik worden maatregelen/ sancties jegens de overtreder genomen.
De universiteit hecht er aan dat de gebruikers van de ICT-voorzieningen ook de algemene maatschappelijke normen en waarden respecteren. Om er voor te zorgen dat de elektronische communicatie ook in dit opzicht in de juiste banen verloopt is er daarom tevens een model-netiquette regeling opgesteld naast dit gebruiksreglement. Daarin zijn in 11 vuistregels een aantal gedragsnormen voor het gebruik van ICT-middelen en -voorzieningen opgenomen.

Artikelsgewijs

Artikel 2

Uitgangspunt is dat de ICT-voorzieningen worden aangeboden ten bate van het onderwijs, onderzoek en de algemene bedrijfsvoering van de Universiteit Utrecht. Dit betekent dat de ICT-middelen en voorzieningen primair bedoeld zijn voor het uitvoeren van de functie binnen de UU, of bij studenten, het volgen van onderwijs.
Persoonlijk gebruik is toegestaan. Daarbij geldt wel te allen tijde de voorwaarde dat het privé-gebruik niet storend mag zijn voor de dagelijkse werkzaamheden van de gebruiker. Medewerkers hebben daarbij een eigen verantwoordelijkheid, waarbij de leidinggevende uiteindelijk beoordeelt of hiervan (nog) sprake is. Tevens geldt de voorwaarde dat het privé-gebruik niet storend mag zijn voor anderen. Er kan bijvoorbeeld sprake zijn van storend gebruik bij het downloaden of versturen van zeer grote bestanden, waardoor een groot beslag wordt gelegd op het universitaire netwerk.

Artikel 3
Aan het gebruik van de ICT-middelen zijn risico's verbonden die nopen tot het stellen van gebruiksregels. Bij risico's valt te denken aan:

- beveiligingsrisico's zoals beschadiging van de ICT-infrastructuur door virussen, bieden van openingen voor computercriminaliteit.
- juridische risico's zoals het maken van inbreuk op intellectueel eigendom van een ander door illegaal downloaden, het downloaden van kinderporno en belediging of discriminatie.
- ethische risico's zoals het in diskrediet brengen van de goede naam van de universiteit of anderen
- kosten: het oneigenlijk gebruik zelf van communicatiemiddelen brengt onnodige kosten met zich mee; verder bestaat een reëel risico van schadeclaims door gedupeerden.
- uitval van systemen en overbelasting van de ICT-infrastructuur: ongewenste toepassingen kunnen het normaal functioneren van diverse systemen binnen het bedrijf ernstig verstoren.

In artikel 3 is daarom in z'n algemeenheid opgesomd welk gebruik verboden is, namelijk gebruik dat:

a) inbreuk maakt op wet- en regelgeving. Gebruik van de ICT-voorzieningen moet uiteraard binnen de grenzen van de wet plaatsvinden. Dat betekent bijvoorbeeld dat illegaal kopiëren van software of het gebruiken van illegaal gekopieerde software niet is toegestaan.
b) beheer, onderhoud, beveiliging, integriteit, kwaliteit en continuïteit van de door de UU aan haar gebruikers aangeboden dienstverlening in gevaar brengt. De integriteit kan bijvoorbeeld in gevaar komen als er illegaal data worden veranderd in een systeem (zoals cijfers van studenten in OSIRIS). De continuïteit kan in gevaar komen als de webserver of een website gebombardeerd wordt met data (denial-of-service attack).
c) de bedrijfsprocessen van de UU verstoort. Het primaire proces en de bedrijfsvoering van de Universiteit Utrecht mogen nimmer in gevaar komen of verstoord worden. Daarvan kan bijvoorbeeld sprake zijn als door het versturen van extreem grote hoeveelheden e-mail het gebruik van de universitaire computersystemen bemoeilijkt of zelf onmogelijk wordt.
d) de UU, gebruikers en/of derden financiële of imagoschade toebrengt. Het is niet toegestaan activiteiten te ontplooien die dit tot gevolg hebben.

Naast de algemene verbodsbepaling is in artikel 3 een opsomming gegeven met voorbeelden van niet toegestaan gebruik. Zo is het verboden met andermans naam gebruik te maken van ICT-middelen en –voorzieningen: het is niet toegestaan toegangsgegevens van andere gebruikers af te vangen of heimelijk te gebruiken. Omgekeerd mogen de persoonlijke inlogcodes ook niet aan anderen bekend worden gemaakt. Omgekeerd mogen de persoonlijke inlogcodes ook niet aan anderen bekend worden gemaakt. Inlogcodes zijn persoonlijk. Bij afwezigheid van een medewerker wegens ziekte kan het noodzakelijk zijn dat de informatie achter een inlogcode (zoals e-mail), geraadpleegd wordt door collega' s of door de leidinggevende. Hierover worden conform het verzuimprotocol afspraken gemaakt tussen leidinggevende en medewerker. Zie (http://www.uu.nl/NL/Informatie/medewerkers/arbeidsvoorwaarden/Documents/Verzuimprotocol.pdf)
Verder mogen medewerkers, gebruikers en studenten de ICT-middelen en -voorzieningen niet inzetten voor privé doeleinden met een commercieel karakter, omdat de software- en internetconnectie-licenties die de universiteit heeft afgesloten commercieel gebruik niet toestaan. Dit neemt niet weg dat de UU ondernemerschap onder studenten wel stimuleert. In het onderwijs is aandacht voor het opzetten van een eigen onderneming. Daarnaast wordt via het Centrum voor Ondernemerschap en Innovatie voorzien in ondersteuning en informatie voor startende ondernemers, onderzoekers en studenten.

Artikel 5
De UU zal de naleving van de regels van het gebruiksreglement controleren. De controle op naleving van de regels vindt niet continu plaats, maar steekproefsgewijs.
Het beleid t.a.v. de controle op gebruik van de door de UU ter beschikking gestelde ICT-middelen is als volgt:

- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een persoon ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden.
- Controle beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.
- Werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.

- E-mailberichten van medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer.

Indien er aanwijzingen zijn dat een persoon of een groep personen de regels overtreedt, kan gedurende een vastgestelde periode gerichte controle plaatsvinden. Hierbij is er sprake van maatwerk waarbij de omvang van de controle zo beperkt mogelijk wordt gehouden. Dit is in overeenstemming met de privacywetgeving.
De registratie van het gebruik van ICT-middelen hoeft niet te worden gemeld bij het College Bescherming Persoonsgegevens (CBP). Deze valt onder het Vrijstellingsbesluit.

Artikel 6
Bij handelen in strijd met dit gebruiksreglement kan het college van bestuur of de mandataris een sanctie opleggen. De sanctie moet altijd in verhouding staan tot het geconstateerde misbruik.
Er is daarbij geen vaste sanctie per soort overtreding. Het college van bestuur/ de mandataris zal bezien:

a. wat de ernst van de bewuste overtreding(en) is,
b. in welke tijdspanne en frequentie de overtreding(en) voorkwamen
c. wat de gevolgen van de overtreding(en) en de hoogte van de eventuele ontstane materiële en immateriële schade zijn.

Aan de hand daarvan zal het college van bestuur/ de mandataris de vorm en de hoogte van de op te leggen sanctie vaststellen. De sancties kunnen bestaan uit:

- al dan niet tijdelijke beperkingen in de toegang tot bepaalde ict-/telefoonfaciliteiten,
- een tijdelijk of definitief verbod tot het gebruik van bepaalde voorzieningen,
- het verhalen van kosten voortvloeiend uit het geconstateerde misbruik of
- (bij medewerkers) het beëindigen van de aanstelling dan wel (bij andere gebruikers) de overeenkomst op grond waarvan de gebruiker toegang had tot de voorzieningen.

Ook andere maatregelen zijn mogelijk, zo lang ze maar passend zijn. Een voorbeeld ter verduidelijking. Een student die via zijn mailbox bulkmail verstuurt zonder dat dit noodzakelijk is in verband met een studieopdracht zal een waarschuwing krijgen dit onmiddellijk te staken. Indien daar niet op gereageerd wordt of indien er sprake is van herhaling, zal het gebruik van de mailbox (voor een bepaalde periode) geblokkeerd worden. Toegang tot de elektronische leeromgeving zal niet beperkt worden, om het studeren niet onmogelijk te maken.

Maatregelen jegens medewerkers kunnen worden genomen op grond van de artikelen 6:12 en 6:15 CAO en de universitaire regeling Orde- en disciplinaire maatregelen (zie bijlage). Tegen een desbetreffend besluit kan de medewerker bezwaar aantekenen bij het college van bestuur en eventueel beroep instellen bij de rechtbank.
Maatregelen jegens studenten vinden hun grondslag in artikel 7.57h van de WHW (zie bijlage). De ontzegging van de toegang tot gebouwen of voorzieningen wordt daar in tijd beperkt tot ten hoogste een jaar. Studenten kunnen tegen een dergelijk besluit bezwaar aantekenen bij het college van bestuur en eventueel beroep instellen bij het College van beroep voor het hoger onderwijs.
Maatregelen jegens overige gebruikers zijn niet gebaseerd op een specifieke (wettelijke) regeling. Voor zover daarover niets is geregeld in de overeenkomst op grond waarvan de gebruiker toegang heeft gekregen tot de universitaire voorzieningen, vloeit het recht om op te treden tegen misbruik voort uit het eigendomsrecht van de universiteit. In dit geval is er geen mogelijkheid van bezwaar of beroep, tenzij daarover expliciet iets is geregeld in de overeenkomst.

Bijlage: Relevante regelingen en bepalingen

Regeling Orde- en disciplinaire maatregelen (zie ook hoofdstuk 6, paragraaf 2 van de CAO NU)

Ordemaatregelen (zie ook artikel 6.15 van de CAO NU)
Ontzegging toegang gebouwen en terreinen

1. De mandataris met het personeelsmandaat is bevoegd in het belang van de universiteit aan de werknemer als ordemaatregel de toegang tot gebouwen, lokalen of terreinen te ontzeggen. De maatregel kan onder meer worden toegepast:
   a. wanneer het ongewenst wordt geacht dat de werknemer komt op plaatsen waar hij voor de uitoefening van zijn functie niet behoeft te komen;
   b. ter voorkoming van verstoring van de rust en orde ter plaatse;
   c. ter voorkoming van (ongewenste) contacten tijdens strafprocedures en daaraan eventueel voorafgaand onderzoek.
2. De ontzegging van de toegang dient schriftelijk en gemotiveerd aan de werknemer te worden medegedeeld onder vermelding van plaats(en) en tijd waarvoor de ontzegging geldt.
3. De ontzegging van de toegang geschiedt voor een aan te geven periode van ten hoogste één maand. De ontzegging kan telkens met ten hoogste één maand worden verlengd.

Disciplinaire maatregelen (zie ook artikel 6.12 en 6.13 CAO NU)

4. Het College van Bestuur kan de bevoegdheid tot het opleggen en ten uitvoer brengen van disciplinaire maatregelen mandateren.
5. Van het onder 4. bedoelde mandaat is uitgezonderd de bevoegdheid tot het opleggen van disciplinaire maatregelen aan hoogleraren en directeuren van de centrale diensten.
6. Ondermandaat van de onder 4. bedoelde bevoegdheid is niet toegestaan.
7. Voorafgaand aan het nemen van een besluit tot opleggen van een disciplinaire maatregel dient advies ingewonnen te worden bij de afdeling Juridische Zaken van de Bestuursdienst.
8. Behalve in geval van een schriftelijke berisping, kan bij de oplegging van een disciplinaire maatregel worden bepaald dat de maatregel onder bepaalde voorwaarden niet ten uitvoer zal worden gelegd. De voorwaarden en de looptijd dienen in het besluit te worden opgenomen.
9. Indien een maatregel is opgelegd die tijdelijk of blijvend een negatief effect heeft op het salaris kan - zo het verdere gedrag van de werknemer daartoe aanleiding heeft gegeven - zijn positie met ingang van een bepaald tijdstip geheel of ten dele in overeenstemming worden gebracht met de positie, zoals deze zonder oplegging van de disciplinaire maatregel zou zijn geweest.
10. Indien een situatie als genoemd in artikel 6.13 CAO zich voordoet, stelt het College van Bestuur dan wel de mandataris een commissie ad hoc in. Dit kan de commissie als bedoeld in 8.9 CAO NU zijn.

Procedure tot oplegging van disciplinaire maatregel

11. Een disciplinaire maatregel kan eerst worden opgelegd, nadat de werknemer in de gelegenheid is gesteld zich te verantwoorden. Bij zijn verantwoording kan hij zich laten bijstaan door een raadsman.
12. De verantwoording geschiedt ten overstaan van (één van de leden van) het College van Bestuur dan wel de mandataris. De werknemer wordt in de gelegenheid gesteld zich mondeling te verantwoorden. Indien de werknemer daaraan de voorkeur geeft, kan hij zich ook schriftelijk verantwoorden. Op zijn verzoek wordt aan de werknemer gelegenheid gegeven zijn schriftelijke verantwoording mondeling alsnog nader toe te lichten.
13. Van de mondelinge verantwoording wordt binnen drie werkdagen een verslag opgemaakt, dat voor akkoord wordt getekend door de werknemer en degene te wiens overstaan de verantwoording heeft plaatsgevonden. Weigert de werknemer de ondertekening, dan wordt daarvan in het verslag melding gemaakt, zo mogelijk met vermelding van redenen. Een afschrift van het verslag wordt aan de werknemer uitgereikt of per aangetekend schrijven verzonden.
14. Ter bevordering van een vlugge en juiste afdoening van voorstellen tot het opleggen van een disciplinaire maatregel dienen in deze voorstellen zoveel als mogelijk de navolgende punten verwerkt te zijn:
   a. persoonlijke gegevens (naam, voorletters, functie en dienstverband van werknemer);
   b. omschrijving van het plichtsverzuim, voor zover nodig toegelicht in een nauwkeurige omschrijving van het oordeel over het gebeurde;
   c. van belang zijnde omstandigheden die naar het oordeel van de mandataris van invloed kunnen zijn geweest; particuliere omstandigheden, waarvan vermelding van belang wordt geacht, zoals eventuele financiële moeilijkheden van de werknemer, ziekte in het gezin, studie kinderen e.d.: uitvoerige beoordeling van de functievervulling, het gedrag enz. van de werknemer en, indien een of ander te wensen overlaat, vermelding of deze op zijn tekortkomingen is gewezen;
   d. vermelding of de universitaire bewakingsdienst is ingeschakeld;
   e. eventueel door de politie c.q. justitie getroffen maatregelen zoals arrestatie (met datum en uur), instellen van een vervolging;
   f. eventuele reeds getroffen ordemaatregelen (non-activiteit; ontzegging toegang);
   g. eventueel de omvang van de door de UU geleden schade en de eventuele inhouding van salaris/bezoldiging;
   h. verdere bijzonderheden die van belang kunnen zijn voor een juiste behandeling van de kwestie of waarvan melding om andere redenen van belang wordt geacht;
   i. oordeel of deze situatie aanleiding geeft de bedrijfsarts of de Taakgroep Veiligheid en milieu in te schakelen en zo ja, of dit reeds is gebeurd;
   j. voorstel tot het treffen van bepaalde maatregelen, met motivering;
   k. (indien het College van Bestuur dan wel de mandataris hiertoe aanleiding aanwezig acht) de nodige gegevens ter beantwoording van de vraag of een besluit tot inhouding van salaris tijdens schorsing, in verband met de sociale omstandigheden van de betrokkene en/of zijn gezin, tot onbillijkheid zou leiden (eventueel rapport bedrijfsmaatschappelijk werk bijvoegen).
15. Het besluit tot oplegging van een disciplinaire maatregel van het College van Bestuur geschiedt schriftelijk en dient met redenen te zijn omkleed. Dit besluit dient onverwijld aan betrokken werknemer te worden gezonden bij aangetekend schrijven met bericht van ontvangst.
16. In het personeelsdossier van de werknemer wordt het besluit tot oplegging van een disciplinaire maatregel opgenomen alsmede de correspondentie die tot dit besluit heeft geleid.

Deze regeling treedt in werking op 10 oktober 2007 en vervangt de voorgaande regeling Orde- en disciplinaire maatregelen.

CAO Nederlandse Universiteiten

Artikel 6.12 Disciplinaire maatregelen
1 De werkgever kan aan de werknemer die zich aan plichtsverzuim schuldig maakt een disciplinaire maatregel opleggen welke in verhouding staat tot het plichtsverzuim.
2 Plichtsverzuim omvat zowel het overtreden van enig voorschrift als het doen of nalaten van iets, wat een goed werknemer in gelijke omstandigheden behoort te doen of na te laten.
3 De werkgever kan met betrekking tot het opleggen van een disciplinaire maatregel nadere regels vaststellen.

Artikel 6.15 Non-activiteit
1 Onverminderd de regels rond het opleggen van een disciplinaire maatregel, zoals genoemd in artikel 6.12 van dit hoofdstuk, kan de werkgever de werknemer op non-actief stellen:
a als een strafrechtelijke vervolging met betrekking tot een misdrijf tegen hem is ingesteld;
b wanneer de werkgever hem op de hoogte heeft gesteld van het voornemen hem in het kader van een disciplinaire maatregel onvoorwaardelijk ontslag te geven, dan wel wanneer hem die maatregel (reeds) is opgelegd;
c wanneer, naar het oordeel van de werkgever, het belang van de instelling dit vereist.
2 Het besluit waarbij de werknemer op non-actief wordt gesteld, vermeldt de datum van ingang daarvan en de omstandigheden die daartoe aanleiding hebben gegeven.

Wet hoger onderwijs en wetenschappelijk onderzoek

Artikel 7.57h. Huisregels en ordemaatregelen
Het instellingsbestuur kan voorschriften geven en maatregelen nemen met betrekking tot de goede gang van zaken in de gebouwen en terreinen van de instelling. Die maatregelen kunnen inhouden dat aan degene die de bedoelde voorschriften heeft overtreden, de toegang tot die gebouwen en terreinen geheel of gedeeltelijk voor de tijd van ten hoogste een jaar wordt ontzegd.