Operational Framework

voor het

CERT-RU

Versie: 2.2

Datum: 29-10-2014

DOCUMENTBEHEER

Wijzigingshistorie

Datum	Auteur	Versie	Wijziging tov. vorige versie
01-01-2001	PeOs	1.0	Initieel document, vastgesteld door CVB als onderdeel beveiligingsbeleid.
05-08-2004	PeOs	2.0	Technische revisie KUN-RU
01-11-2012	PeOs	2.1	Technische revisie vorming GDI
29-10-2014	JePo	2.2	Technische revisie UCI en GDI opgegaan in ISC Bevoegdheid tot tijdelijke afsluiting van systemen opgenomen. Vastgesteld door CVB 12-01-2015

Distributie

Datum	Versie	Verzonden aan
01-11-2012	2.1	Directeur UCI, Hoofd GDI, Leden CERT
29-10-2014	2.2	Leden CERT, Directeur ISC, Hoofd BJZ, Secretaris CVB.

Inhoud

1. Introductie

Het RU "Computer Emergency Response Team" (CERT-RU) is in 2001 door het College van Bestuur ingesteld voor het coördineren van het oplossen en voorkomen van incidenten waarmee de Radboud Universiteit kan worden geconfronteerd op het gebied van computer- en netwerk-beveiliging. De instelling, doelstelling en taken van CERT-RU vloeien voort uit de door het College van Bestuur vastgestelde beleidsuitgangspunten[1].

2. Mission statement

Het RU “Computer Emergency Response Team” (CERT-RU) is ingesteld voor het coördineren van het oplossen en voorkomen van incidenten waarmee de RU kan worden geconfronteerd op het gebied van computer- en netwerkbeveiliging.

Beveiliging is naar wijze van aangrijpen in te delen in de deelterreinen:

- preventie
- detectie
- risico-beheersing
- correctie
- repressie

CERT-RU richt zich primair op de coördinatie van detectie en correctie, dat wil zeggen op de coördinatie van signalering en afhandeling van beveiligingsincidenten.
Aan preventie draagt CERT-RU bij door algemene voorlichting en aanbevelingen ten aanzien van kwetsbaarheden en bedreigingen.
In voorkomende gevallen kan CERT-RU actief aan risicobeheersing doen door services of systemen tijdelijk te laten afsluiten.
Repressie en correctie is een verantwoordelijkheid van de eigenaar van het betreffende ICT-bedrijfsmiddel: ISC, Domeineigenaren, Faculteiten, Clusters, Onderzoeksinstituten e.d..

CERT-RU heeft de opdracht:

- beveiligingsincidenten te signaleren, te coördineren bij bestrijding ervan en toe te zien op adequate en tijdige oplossing van problemen die tot incidenten hebben geleid of door incidenten zijn veroorzaakt (c.q. waar nodig bij de oplossing ondersteuning te bieden);
- beveiligingsincidenten direct te escaleren wanneer:
    - reputatie- of imagoschade voor de universiteit aan de orde kan zijn; escalatie vindt plaats naar de secretaris van het College van Bestuur dan wel naar de aandachtsvelder ICT binnen het College
    - de afhandeling van een incident onaanvaardbare vertraging oploopt, zulks ter beoordeling van CERT-RU; escalatie vindt dan in eerste instantie via de lijnorganisatie plaats
- voorlichting te geven (algemene aanbevelingen doen aan systeembeheerders en gebruikers door verspreiden van informatie)
- bij landelijke of grootschalige malware-uitbraken het management van de universiteit te informeren over de stand van zaken bij de RU.

[1] Zie de actuele versie van de Beleidsnotitie Informatiebeveiliging

3. Diensten

CERT-RU levert de volgende primaire diensten:

3.1. Coördinatie van beveiligingsincidenten

Dit houdt in het onderhouden van een meldpunt voor beveiligingsincidenten (detectie), als vervolg daarop het coördineren van de afhandeling van die beveiligingsincidenten (correctie), en zonodig het assisteren in de zin van gegevensverstrekking aan partijen binnen de RU die tot repressie willen overgaan. Ook het escaleren van incidenten naar het CvB of de lijnorganisatie valt hieronder. Contacten met politie en justitie (informeren of aangifte) zullen door CERT-RU in principe niet zelfstandig gelegd worden. Wanneer politie en/of justitie zelf contact opneemt met CERT-RU zal BJZ ingeschakeld worden.

De contactpersonen voor de coördinatie van incidenten zijn binnen de RU de Domain Security Contacts (DSC's), en buiten de RU andere CERT teams, vooral Surf-CERT. Iedereen buiten de RU kan overigens incidenten melden bij CERT-RU. In principe geldt hetzelfde voor alle gebruikers binnen de RU, zij het dat aangemoedigd zal worden dat gebruikers incidenten melden via de bestaande ondersteuningskanalen.

3.2. Voorlichting over incidenten en actuele bedreigingen

Deze voorlichting houdt in het binnen de RU aanhangig maken van actuele security vulnerabilities en de oplossingen daarvoor, zo mogelijk toegespitst op binnen de RU in zwang zijnde systemen en netwerken.
De verspreiding van voornoemde informatie gaat actief naar de DSC's binnen de RU, en passief via publicatie op de ICT-beveiligingssite van de RU Nijmegen (http://www.ru.nl/ict-beveiliging)
Bronnen van informatie zijn, naast vrije nieuwsgaring van de CERT-RU leden, vooral het Upstream CERT en de advisory distributielijsten van een aantal voor de RU relevante leveranciers en dienstverleners.
Het informeren van het management van de universiteit bij landelijke of grootschalige malware-uitbraken over de stand van zaken bij de RU Nijmegen valt hier ook onder.

3.3. Advisering ten aanzien van RU ICT beveiligingsaspecten en -beleid

CERT-RU kan gevraagd en ongevraagd advies uitbrengen aan eigenaren en beheerders van ICT-bedrijfsmiddelen dat tot doel heeft RU-specifieke beveiligingsproblemen te helpen oplossen of verminderen. Advies zal altijd, naast het signaleren van een beveiligingsprobleem, ook concrete aanbevelingen bevatten om de risico's te verkleinen en het probleem op te lossen.

4. Vertrouwelijkheid

Communicatie met CERT-RU vindt plaats op basis van vertrouwelijkheid. CERT-RU zal dan ook geen inhoudelijke informatie over incidenten of de melders daarvan aan derden verstrekken. Informatie over beveiligingsincidenten wordt alleen doorgegeven aan betrokken partijen voor zover relevant en noodzakelijk voor de oplossing van een incident.

5. Organisatie

5.1. Verantwoordelijkheden en bevoegdheden van CERT-RU

De verantwoordelijkheden van CERT-RU zijn weergegeven in het Mission Statement. CERT-RU beschikt niet over bevoegdheden die verder reiken dan het eigen functioneren, met uitzondering van bevoegdheden voor risiscobeheersing. Risicobeheersing houdt in dat bij acute beveiligingsincidenten met een groot risico die niet adequaat afgehandeld worden CERT-RU kan overgaan tot het (tijdelijk) laten afsluiten van services of systemen, Nadrukkelijk wordt gesteld dat correctie en repressie niet tot de taken van CERT-RU behoort: CERT-RU heeft daartoe niet de benodigde lokale autoriteit, en zou bovendien met een dergelijke taak niet in staat zijn binnen de RU de gewenste onafhankelijkheid en reputatie van betrouwbaarheid te verwerven die cruciaal zijn voor een CERT.

5.2. Doelgroep

CERT-RU werkt voor de RU als geheel, en in het bijzonder voor de IM-eenheden waaruit de Universiteit is opgebouwd. Beveiligingsincidenten kunnen in principe door iedereen gemeld worden. Binnen de universiteit wordt echter aangemoedigd dat melding plaatsvindt via de bekende ondersteuningskanalen, die via de DSC doormelden naar CERT-RU, tenzij lokale afhandeling triviaal is. CERT-RU handelt in beginsel alle communicatie af via de DSC's, tenzij een dergelijke afhandeling in strijd is met de privacy van een individuele melder. Buiten de universiteit wordt het Upstream CERT gebruikt als primaire communicatiepartner – andere CERT's of ISP's kunnen echter wel incidenten melden bij CERT-RU.

5.3. Samenstelling CERT-RU

CERT-RU bestaat uit een beperkt aantal (5-10) personen die beschouwd worden als deskundigen op het gebied van computer- en netwerkbeveiliging. De CERT-RU leden hebben bovendien goede kennis van de structuur en de werking van de RU-organisatie. De RU Security Officer (voorzitter) en de ISC-Securitymanager (secr.) zijn qualitate-qua lid van CERT-RU.

5.4. Lidmaatschap CERT-RU

Het lidmaatschap van CERT-RU vereist competentie op het gebied van computer en netwerk-beveiliging, ervaring en een uitgebreid netwerk, met als enig doel CERT-RU te helpen effectief zijn taak te kunnen verrichten. Het medewerker zijn van de RU is de enige randvoorwaarde. In geval van vacatures zal CERT-RU een kandidaat voorstellen aan de Directeur ISC en het lijnmanagement van de betreffende kandidaat. Benoeming vindt plaats door de Directeur ISC op voordracht van het betreffende lijnmanagement. Benoeming
houdt in alle gevallen de erkenning in dat de bewuste medewerker een deel van zijn tijd zal besteden aan CERT-RU werk, en de erkenning dat bij ernstige incidenten dat werk een hoog prioriteitsgehalte heeft. Het werk als CERT-lid kent een hoog volontair gehalte. Het functioneren als team met de daarbij behorende essentiële attributen zullen de continuïteit van CERT-RU in de praktijk moeten borgen.

5.5. Verantwoording

De rapportage over de werkzaamheden van CERT-RU maakt deel uit van de rapportage die de Security Officer van de RU Nijmegen eens per kwartaal aan het CvB uitbrengt.
Budgetbehoefte wordt door het CvB via het managementcontract met het ISC afgedekt.

5.6. Faciliteiten en voorzieningen

Het ISC stelt vergaderruimte en technische faciliteiten beschikbaar. CERT-RU kan gebruik maken van het NOC-ISC gedurende de openingstijden.
Tevens heeft CERT-RU een budget waaruit voor de CERT-RU-leden een onkostenvergoeding betaald kan worden.

5.7. Interne organisatie

CERT-RU kan voor aangelegenheden betreffende computer- of netwerkbeveiliging werkgroepen instellen. CERT-RU stelt tijdens een vergadering opdracht, samenstelling en werkwijze van een werkgroep vast. In een werkgroep kunnen naast leden ook externe deskundigen deelnemen. Werkgroepen zijn verantwoording schuldig aan CERT-RU. Resultaten van werkgroepen hebben de status van advies aan CERT-RU.
De Directeur ISC kan een lid van CERT-RU dat zich niet houdt aan algemene regels, zoals die onder meer in dit document zijn vastgelegd, of niet meewerkt aan doel en opdracht van CERT-RU, of de goede naam van CERT-RU of de RU bezoedelt, als lid royeren. CERT-RU wordt daarvoor gehoord voor advies.

5.8. Organisatorische inbedding van CERT-RU in de RU

Elke eenheid en elk informatiedomein binnen de doelgroep van CERT-RU wordt geacht voor communicatie met CERT-RU een vaste DSC (Domein Security Contact) functie in te richten die zorg draagt voor rapportage en afhandeling van incidenten en het treffen van maatregelen binnen de eigen beheerorganisatie, daaronder ook begrepen preventieve maatregelen en voorlichting van de eigen gebruikers. De DSC is bij voorkeur de directeur bedrijfsvoering van een IM-eenheid of de domeineigenaar van een informatiedomein.

De DSC functie vereist continuïteit. De DSC dient dan ook zorg te dragen voor een operationeel aanspreekpunt tijdens kantooruren. Het secretariaat van CERT-RU houdt een lijst bij van deze functionarissen, hun functionele e-mail adressen en telefoonnummers. CERT-RU stelt de DSC functionarissen op de hoogte van de voor hen relevante informatie.

5.9. Organisatorische inbedding van CERT-RU buiten de RU

CERT-RU vestigt en onderhoudt een vaste operationele werkrelatie met zijn Upstream CERT en heeft langs die weg korte verbindingen met andere bestaande CERT's. Dit is belangrijk voor de informatie-uitwisseling, een kritische factor voor de effectiviteit van een CERT. De voorzitter van CERT-RU vertegenwoordigt CERT-RU formeel bij het Upstream CERT en andere CERT's.

Het Upstream CERT dient FIRST-lid te zijn, daarmee CERT-RU vrijwarend van de noodzaak van FIRST lidmaatschap. De jaarlijkse FIRST conferentie is voor CERT-RU een aangewezen mogelijkheid tot kennisverbreding en -verdieping.

CERT-RU registreert zich als Level 0 team in TI kader

CERT-RU is vertegenwoordigd in het landelijk overleg van HO-CERTs (SCIRT).

CERT-RU voert geen directe communicatie met de pers. Alle contacten met de pers verlopen via de woordvoerder van de Universiteit. De voorzitter van CERT-RU onderhoudt daartoe zo nodig

contact met de woordvoerder. De Directeur ISC en daarmee het CvB, en CERT-RU worden door de woordvoerder op de hoogte gehouden van contacten met de pers die CERT-RU aangaan.

6. Meldpunt en contactinformatie

6.1. Bereikbaarheid

Het NOC-ISC fungeert tijdens openingstijden voor CERT-RU als het telefonisch meldpunt voor incidenten. CERT-RU is voor algemene aangelegenheden via het CERT-secretariaat te bereiken.

Voor alle personen die tot de doelgroep van CERT-RU behoren, evenals voor het Upstream CERT en andere CERT's is CERT-RU bereikbaar:

Melding CERT-RU incidenten	Overige zaken via CERT-RU secretariaat
• Per telefoon aan het meldpunt (024-36)10818 • Per e-mail aan de CERT-medewerker van dienst via cert@ru.nl, abuse@ru.nl, security@ru.nl of sep@ru.nl	• Per e-mail:H.Harings@ru.nl • Per telefoon:024-38187538 • Schriftelijk: Geert Grooteplein 41, 6525 GA Nijmegen

Voor communicatie met CERT-RU dient te worden aangesloten bij het urgentieniveau van de communicatie:

- **Standaard**: communicatie met CERT-RU via e-mail (of in bijzondere gevallen per fax) verdient in het algemeen de voorkeur. Op deze berichten zal steeds binnen 24 uur worden gereageerd.
- **Urgent**: meldingen telefonisch via het NOC-ISC onder vermelding van CERT-URGENT. De medewerkers van het NOC-ISC zijn geïnstrueerd in het aannemen van gesprekken voor CERT-RU en het doorgeleiden van urgente meldingen naar de CERT-RU medewerker van dienst.

De voorzitter van CERT-RU is verantwoordelijk voor het handhaven van de goede bereikbaarheid en voor het bekendmaken van de verschillende mogelijkheden om CERT-RU te bereiken.

6.2. Technische voorzieningen

Telefoon en fax

De telefoon van CERT-RU-meldpunt is die van het NOC-ISC. De CERT medewerker van dienst dient te beschikken over een mobiele telefoon.

Registratiesysteem

Voor de registratie van incidenten en het volgen van de afhandeling beschikt CERT-RU over een eigen administratie. Deze administratie wordt door de CERT medewerker van dienst bijgewerkt en bij de dienstoverdracht via e-mail doorgestuurd.

E-mail

Ten behoeve van de veilige uitwisseling van incident gerelateerde informatie wordt secure e-mail gebruikt wanneer nodig. Hiertoe stelt CERT-RU een public PGP-key ter beschikking voor encrypted mail naar CERT-RU; verder heeft CERT-RU een key om uitgaande mail te signeren, en hebben alle CERT-RU leden zelf PGP(-achtige) voorzieningen.

7. Fundamentele Policies

De volgende fundamentele policies zijn voor CERT-RU van kracht:

a. Security Policy
b. Pers/PR Policy
c. Code of Conduct

Policies zijn richtinggevende beginsels en prevaleren daarmee altijd boven procedures: policies kunnen wel hun operationele uitwerking vinden in procedures.
De policies worden hieronder uitgewerkt voorzover nodig in het kader van dit operational framework:

7.1. Security Policy

CERT-RU houdt zich bezig met het coördineren van veiligheidsincidenten. Dergelijke incidenten kunnen naast relatief “onschuldige” zaken ook bedrijfs- of onderzoeksgeheimen betreffen, laster-campagnes of onwelvoeglijke uitingen, strafbaar gedrag in alle gradaties, enzovoorts.

Derhalve dient CERT-RU zich te allen tijde bewust te zijn van de potentiële grote gevoeligheid van zijn taak, en dus alle voorzorgen nemen op het gebied van veiligheid zodat CERT-RU zelf nooit deel van het probleem kan worden. Hoogste gebod voor CERT-RU is zelf niet betrokken te raken bij incidenten, maar alleen als bemiddelaar te blijven dienen.

De security policy van CERT-RU is er op gericht om te allen tijde te voorkomen dat CERT-RU nalatigheid kan worden verweten.

Nalatigheid in de ruimste zin des woords, niet alleen betreffende vertrouwelijkheid en integriteit, maar ook betreffende het element van beschikbaarheid: immers een CERT die niet (tijdig) reageert pleegt ook een inbreuk op de veiligheid die het betracht ten aanzien van zijn taak.

De security policy van CERT-RU valt in twee delen uiteen, een intern en een extern deel:

- het interne deel betreft de manier waarop CERT-RU zichzelf beveiligt, qua communicatie, opslag van gegevens, enzovoorts. Daarbij worden de volgende uitgangspunten gehanteerd:
  - beveiliging van communicatie en data-opslag volgens *best current practices* voor CERTs
  - *versleuteling* van gegevens waar nodig
  - *alleen* CERT-RU leden hebben toegang tot gegevens
  - rapportages e.d. vinden plaats onder *anonimisering* van de incidenten

- het externe deel betreft de manier waarop CERT-RU met de informatie omgaat die het van buiten krijgt, vooral in het kader van incidenten: deze zogenaamde “information handling policy” is integraal onderdeel van de interne security policy maar daarnaast expliciet te vinden op de CERT-RU website als onderdeel van CERT-RU profiel conform RFC-2350. Daarbij zijn de volgende uitgangspunten gehanteerd:
  - alle binnenkomende informatie wordt *vertrouwelijk* behandeld, ongeacht de prioriteitstelling

- evident zeer gevoelige informatie of informatie die door de informatieverstrekker expliciet als dusdanig wordt aangemerkt wordt bovendien uitsluitend *versleuteld* gecommuniceerd
- CERT-RU behoudt zich het recht voor om in het kader van de afhandeling van een incident gebruik te maken van verstrekte informatie: dit gebeurt echter alleen *op need-to-know basis*, en in principe *in geanonimiseerde vorm*
- als een informatieverstrekker aanvullende beperkingen verbindt aan het verspreiden van de bewuste informatie, zal CERT-RU dat respecteren: als het betekent dat CERT-RU daardoor in feite niet kan handelen op een zaak zal CERT-RU dat expliciet vermelden
- CERT-RU doet geen aangifte van incidenten bij justitie, tenzij de wet dat vereist (wat het geval is bij ernstige misdrijven of de verdenking daarvan): CERT-RU is namelijk geen partij in incidenten, maar bemiddelaar
- CERT-RU werkt in principe op verzoek van justitie mee in officiële onderzoeken: zo'n verzoek wordt altijd eerst voorgelegd aan BJZ en het advies van BJZ wordt opgevolgd.

7.2. Pers/PR Policy

CERT-RU leden hebben tot taak om veiligheidsincidenten te helpen oplossen: deze taak vereist bij ernstige incidenten grote concentratie, en heeft een sterk real-time karakter. Andere taken dienen daarom door de ter zake kundigen te worden afgehandeld. Derhalve is de pers/PR policy voor CERT-RU:

Alle vragen over CERT-werk gesteld door de pers of in het kader van PR worden verwezen naar en afgehandeld door de persvoorlichter/woordvoerder van de RU.

7.3. Code of Conduct

In algemene zin geldt voor CERT-RU als code-of-conduct:

CERT-RU leden spreken namens CERT-RU en gedragen zich in het kader van hun functie te allen tijde geduldig, waardig en beheerst.

8. Procedure dienst 'coördinatie van beveiligingsincidenten'

Zie "Procedures voor incidentafhandeling door CERT-RU; deel 2: Procedure voor de CERT medewerker van dienst."

9. Procedure dienst 'voorlichting over incidenten en actuele bedreigingen'

Voorlichting zal voorlopig op drie verschillende manieren gegeven worden:

a. Eén op één doorgeven van advisories van derden aan direct belanghebbenden.

b. Het uitbrengen van eigen advisories.
In bijzondere gevallen kan CERT-RU zelf besluiten een advisory te doen uitgaan.

c. De CERT-RU website.
Bereikbaar onder http://www.ru.nl/CERT.

10. Procedure dienst 'advisering ten aanzien van RU ICT beveiligingsaspecten'

CERT-RU kan gevraagd en ongevraagd advies uitbrengen over ICT beveiligingsaspecten.
De werkwijze is hierbij als volgt:

- Alleen de DSC's en de CERT-RU leden zelf kunnen de voorzitter verzoeken een advies over een bepaald onderwerp uit te (laten) brengen
- De voorzitter bespreekt dit verzoek met de leden van CERT-RU
- Na instemming wordt een werkgroep gevormd uit de CERT-RU leden
- Die werkgroep wordt zonodig versterkt met enkele materiedeskundigen
- De werkgroep schrijft een (kort) rapport met conclusies en aanbevelingen
- Op basis van dat rapport stelt CERT-RU een advies op dat wordt aangeboden aan de aanvrager en aan de directeur ISC..

Het hiervoor benodigde budget kan uit verschillende bronnen gefinancierd worden:

- Het operationele budget van CERT-RU
- De aanvrager
- Het centrale niveau

11. Amendering Operational Framework

Wijzingen in dit document worden, na advies van CERT-RU, door het College van Bestuur vastgesteld.

Bijlagen.

Bijlage 1: Definities

RU
Onder (de) RU wordt in dit document begrepen alle organisatie-eenheden die ressorteren onder de Radboud Universiteit Nijmegen.

RU: terrein, organisatie en populatie
Met “elektronische informatiesystemen bij de RU” worden de systemen aangeduid die zich binnen de grenzen van onder de RU ressorterende organisatie-eenheden bevinden. Deze systemen en hun gebruikers behoren tot verschillende organisaties (rechtspersonen). Samen vormen deze de doelgroep van CERT-RU.

RU-netwerk
In dit document wordt onder RU-netwerk het geheel verstaan van elektronische informatiesystemen en voorzieningen voor datacommunicatie van de RU.

RU security policy
De voorwaarden verbonden aan het gebruik van het RU-netwerk en SURFnet zijn vastgelegd in het “Reglement RU-netwerk en SURFnet”. Voor toegang tot het RU-netwerk is het onderschrijven van deze policy een voorwaarde. Dit reglement wordt herschreven tot een “Acceptable Use Policy”, waarin de regels die binnen de RU gelden voor het zorgvuldig omgaan met informatie, informatiesystemen en netwerken zijn vastgelegd. Deze policy geldt voor de gehele (doelgroep van CERT-) RU.

RU Security Officer
De RU Security Officer maakt qualitate qua als voorzitter onderdeel uit van CERT-RU.

ISC Security Manager
De ISC Security Manager maakt qualitate qua als secretaris onderdeel uit van CERT-RU.

Beheerders en beheerdomeinen
Ieder informatiesysteem moet een eigenaar en een beheerder hebben. De beheerder is een individuele functionaris die voor één of meer systemen de dagelijkse zorg draagt. Deze zorg is de beheerder opgedragen door of namens de eigenaar van het systeem, op een wijze die past bij de organisatiestructuur van de rechtspersoon die eigenaar is van het systeem. Aansluitend bij die structuur wordt voor het beheer van een aantal systemen binnen een (deel van een) organisatie vaak een gemeenschappelijke beheerorganisatie gevormd. Deze systemen behoren dan tot eenzelfde beheerdomein; vaak valt zo’n beheerdomein samen met een IM-eenheid.
De dienstverlening van CERT-RU is primair gericht op deze beheerdomeinen binnen de RU.

RU-DSC – Domein Security Contact
Een DSC is het aanspreekpunt van een beheerdomein voor alle beveiligingszaken op tactisch en operationeel niveau. Een DSC is bij voorkeur de directeur bedrijfsvoering van een beheerdomein. De real-time aard van ICT beveiligingsincidenten houdt in dat de het operationele deel van de DSC functie niet door één persoon ingevuld kan worden: minimaal binnen kantooruren dient de DSC zorg te dragen voor een operationeel meldpunt voor beveiligingsincidenten. Dit meldpunt wordt bij voorkeur uitbesteed aan de lokale ICT-ondersteuners.

Incident
Een incident is een gebeurtenis of het constateren van een gebeurtenis die een bedreiging vormt of kan vormen voor de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens in elektronische informatiesystemen binnen de RU of in informatiesystemen buiten de RU die met systemen binnen de RU gegevens uitwisselen.

CERT-medewerker van dienst
Voor alarmering en eerste beoordeling van incidenten is altijd (binnen het CERT-RU service window) een lid van CERT-RU beschikbaar. Deze beschikbaarheidsfunctie wordt in dit document aangeduid met CERT-medewerker van dienst.

Upstream CERT
Het Upstream CERT is het CERT van de ISP van de RU. Het Upstream CERT is - bij goed functioneren van deze CERT - de standaard bron en bestemming van incident gerelateerde informatie voor CERT-RU. Thans is Surf-CERT, het CERT voor klanten van SURFnet, het upstream CERT voor de RU. Surf-CERT kent de functie Site Security Contact (SSC): de functionaris die contact onderhoudt met Surf-CERT inzake lopende incidenten. Vanwege de vereiste continuïteit kan de SSC functie niet door één persoon ingevuld worden. De binnen de RU bestaande SSC functie wordt ingevuld door CERT-RU.

TI (Trusted Introducer)
TI (Trusted Introducer) is de trusted repository voor gegevens over Europese CERT teams. Alle bekende teams worden door TI als “Level 0” opgenomen in haar repository. Door aan een aantal voorwaarden te voldoen en uitgebreidere service informatie te verschaffen aan TI, kan een CERT-team in de TI repository worden opgenomen als “Level 2” team. Level-2 teams hebben toegang tot een afgeschermd deel van de repository met de volledige informatie door henzelf en hun collega Level-2 teams verstrekt. Level-2 teams onderhouden in samenspraak met TI de door hen verstrekte informatie, daarmee garanderend dat de TI repository up-to-date blijft. Zie **http://www.trusted-introducer.org/** .

FIRST
FIRST is het internationale Forum of Incident Response and Security Teams (http://www.first.org). FIRST verzorgt informatie uitwisseling en zorgt voor wereldwijde onderlinge erkenning tussen CERT’s.

Bijlage 2: Procedures voor incidentafhandeling door CERT-RU; deel 1: Procedure voor de CERT-RU Helpdesk. (vertrouwelijk)

Bijlage 3: Procedures voor incidentafhandeling door CERT-RU; deel 2: Procedure voor de CERT medewerker van dienst. (vertrouwelijk)

Bijlage 4: Procedures voor incidentafhandeling door CERT-RU; deel 3: Procedure voor de DSC. (vertrouwelijk)