2026 STAATSBLAD VAN DE REPUBLIEK SURINAME No. 94

RESOLUTIE van 09 september 2026 no. 1786/RP, houdende instelling en inwerkingtreding van het Suriname Cyber Security Incident Response Team (SUR-CSIRT).

PRESIDENT VAN DE REPUBLIEK SURINAME,

Gehoord:

- De Veiligheidsadviseur van de President van de Republiek Suriname.
- De Directeur van het Directoraat Nationale Veiligheid.

Gelet op:

- Artikel 99 van de Grondwet van de Republiek Suriname (S.B. 1987 no. 116, zoals laatstelijk gewijzigd bij S.B. 2023 no. 157);
- Wet van 24 december 2017, houdende regels inzake het rechtsverkeer langs elektronische weg (Wet Elektronisch rechtsverkeer) (S.B. 2017 no.86);
- Het "Besluit Taakomschrijving Departementen 1991" (S.B. 1991 no. 58, geldende tekst S.B. 2010 no. 174, zoals laatstelijk gewijzigd bij S.B. 2025 no. 124);
- De Resolutie van 03 april 2024 no. 111/RP, houdende vaststelling van de gewijzigde organisatiestructuur en taakomschrijving van het Directoraat Nationale Veiligheid van het Kabinet van de President van de Republiek Suriname;

- De Resolutie van 29 december 2025 no. 2200/RP, houdende vaststelling van de gewijzigde organisatiestructuur en de taakomschrijving van het Kabinet van de President van de Republiek Suriname;
- Het Nationaal Strategisch Veiligheidsplan 2023–2028;

Overwegende:

- dat internationale standaarden en aanbevelingen oproepen tot de instelling van formeel gemandateerde nationale CSIRT-structuren;
- dat cyberdreigingen zich in toenemende mate ontwikkelen in complexiteit, schaal en impact en daardoor een directe bedreiging vormen voor de nationale veiligheid, de openbare orde en de continuïteit van vitale infrastructuren;
- dat digitale systemen binnen de publieke en private sector sterk onderling verweven zijn, waardoor cyberincidenten zich keten breed en grensoverschrijdend kunnen manifesteren;
- dat een effectieve nationale aanpak van cyberincidenten een gecentraliseerd, deskundig en operationeel gecoördineerd mechanisme vereist voor detectie, analyse, respons en herstel;
- dat het Nationaal CSIRT van de Republiek Suriname sinds 2018 bij de OAS is aangemeld en internationaal geregistreerd staat als Suriname Cyber Security Incident Response Team – SUR-CSIRT;
- dat het Suriname Cyber Security Incident Response Team (SUR-CSIRT), reeds operationeel actief is en verdere formalisering en uitbreiding van mandaat vereist;
- De het SUR-CSIRT onder directe verantwoordelijkheid van de President van de Republiek zal vallen;
- dat met inachtneming van de recente totstandkoming, goedkeuring en aanname van de “UN–Convention against Cybercrime” op 08 augustus 2024, besloten is om het hiernavolgende vast te stellen.

BESLUIT:

I. **Vast te stellen:**

Artikel 1

Begripsbepalingen

1. In deze resolutie wordt verstaan onder:
   a. Cyberincident: een gebeurtenis die de beschikbaarheid, integriteit, authenticiteit of vertrouwelijkheid van een netwerk- of informatiesysteem of de daarin verwerkte informatie daadwerkelijk of potentieel aantast;
   b. Ernstige cyberdreiging: een dreiging waarvan redelijkerwijs kan worden verwacht dat zij aanzienlijke schade veroorzaakt;
   c. Essentiële of vitale dienst: een dienst waarvan verstoring ernstige maatschappelijke, economische, veiligheids- of bestuurlijke gevolgen kan hebben;
   d. Incidentrespons: de technische en organisatorische activiteiten gericht op voorbereiding, detectie, analyse, beheersing, herstel en evaluatie;
   e. NC-CSIRT: de Nationale Coördinator SUR-CSIRT;
   f. Raad: de Nationale Cyberveiligheidsraad;
   g. SUR-CSIRT: het Suriname Cyber Security Incident Response Team.

2. Waar in deze resolutie naar een wettelijke bevoegdheid wordt verwezen, wordt daaronder uitsluitend een bevoegdheid verstaan die op het moment van uitoefening uit de Grondwet, een wet, staatsbesluit of andere geldige regeling voortvloeit.

Artikel 2

Instelling, positie en rechtskarakter

1. Het Suriname Cyber Security Incident Response Team (SUR-CSIRT) wordt ingesteld als nationaal technisch en operationeel coördinatiepunt voor cybersecurity en cyberincidentrespons.

2. SUR-CSIRT ressorteert gedurende de overgangsfase rechtstreeks onder de President en wordt begrotingstechnisch en administratief ondergebracht bij het Kabinet van de President.

3. SUR-CSIRT is geen opsporingsinstantie, vervolgingsinstantie, inlichtingen- of veiligheidsdienst, toezichthouder of zelfstandig bestuursorgaan en verkrijgt door deze resolutie geen strafvorderlijke, sanctionerende of algemene dwangbevoegdheden.

4. De operationele onafhankelijkheid die voor vertrouwelijke en deskundige incidentafhandeling noodzakelijk is, wordt gewaarborgd binnen de verantwoordingslijn aan de President en de toepasselijke wet- en regelgeving.

Artikel 3

Doel en uitgangspunten

1. SUR-CSIRT heeft tot doel de digitale weerbaarheid van de Republiek Suriname te versterken en schade door cyberdreigingen en cyberincidenten te voorkomen, beperken en herstellen.

2. SUR-CSIRT handelt deskundig, risicogestuurd, tijdig, proportioneel, vertrouwelijk, controleerbaar en met minimale verstoring van dienstverlening en grondrechten.

3. Bij de verwerking en uitwisseling van informatie worden doelbinding, dataminimalisatie, noodzakelijkheid, beveiliging, bewaarbeperking en controleerbare autorisatie toegepast.

Artikel 4

Taken van SUR-CSIRT

1. SUR-CSIRT is belast met:
   a. het inrichten van een 24/7 nationaal meld- en contactpunt;
   b. intake, registratie, triage, classificatie, technische analyse, escalatie, coördinatie, herstelondersteuning en evaluatie van cyberincidenten;
   c. het uitgeven van waarschuwingen, dreigingsbeelden, technische adviezen en herstelrichtlijnen;
   d. het ondersteunen van staatsorganen en, op basis van instemming, overeenkomst of wettelijke grondslag, publieke en private beheerders van essentiële of vitale diensten;
   e. het coördineren van beveiligde informatie-uitwisseling;
   f. het ondersteunen van vulnerability management, crisisvoorbereiding, oefeningen, training en bewustwording;
   g. het onderhouden van nationale en internationale CSIRT-samenwerking;
   h. het adviseren van de President en de Regering over cybersecuritybeleid, strategie en noodzakelijke wetgeving; en
   i. het ontwikkelen en beheren van nationale operationele protocollen.

2. SUR-CSIRT kan technische diagnostiek, malware analyse en digitale forensische ondersteuning verrichten voor zover de rechthebbende of bevoegde beheerder daartoe schriftelijke opdracht of toestemming heeft gegeven, of een uitdrukkelijke wettelijke grondslag bestaat.

3. Zodra aanwijzingen van een strafbaar feit bestaan, worden digitale sporen behandeld volgens een met het Openbaar Ministerie en het Korps Politie Suriname afgestemd protocol. De leiding van het strafrechtelijk onderzoek en de strafvorderlijke bevoegdheden blijven uitsluitend bij de wettelijk bevoegde autoriteiten.

4. Internationale vertegenwoordiging geschiedt binnen het door de President of de bevoegde minister vastgestelde buitenlandse beleid en laat verdragsrechtelijke bevoegdheden onverlet.

Artikel 5

Nationale Coördinator SUR-CSIRT

1. SUR-CSIRT staat onder dagelijkse en operationele leiding van de NC-CSIRT, die bij afzonderlijke resolutie door de President wordt benoemd, geschorst en ontslagen.

2. De NC-CSIRT rapporteert rechtstreeks aan de President, adviseert de President over cybersecurity en is voorzitter van de Raad.

3. De NC-CSIRT is verantwoordelijk voor de organisatie, personele en technische gereedheid, veilige bedrijfsvoering, begrotingsvoorbereiding, kwaliteitsborging, internationale samenwerking en rechtmatige uitvoering van de taken van SUR-CSIRT.

4. De NC-CSIRT stelt jaarlijks een werkplan, risicobeeld, begrotingsvoorstel en verantwoordingsrapport op en legt deze aan de President voor.

5. De NC-CSIRT wijst een plaatsvervanger aan die uitsluitend bij afwezigheid of verhindering optreedt en aan dezelfde eisen van deskundigheid, screening en geheimhouding voldoet.

Artikel 6

Presidentieel mandaat en begrenzing

1. De President mandateert de NC-CSIRT om namens en onder verantwoordelijkheid van de President de in deze resolutie omschreven bestuurlijke, technische en coördinerende besluiten te nemen en handelingen te verrichten, voor zover deze behoren tot de uitvoerende bevoegdheid van de President en niet bij of krachtens de wet aan een ander orgaan zijn voorbehouden.

2. Het mandaat omvat in ieder geval:
   a. activering en coördinatie van de nationale cyberincidentrespons;
   b. het verzoeken om operationele medewerking en informatie van onder de uitvoerende macht ressorterende diensten;
   c. het uitvaardigen van technische beveiligingsadviezen en tijdelijke responsinstructies binnen de overheidsdienst;
   d. het bijeenroepen van de Raad; en
   e. het aangaan van operationele samenwerkingsafspraken binnen goedgekeurde beleids- en begrotingskaders.

3. Het mandaat omvat niet:
   a. wetgeving of regelgeving;
   b. strafvorderlijke of opsporingshandelingen;
   c. toegang tegen de wil van een rechthebbende tot locaties, systemen, apparaten of gegevens;
   d. onderschepping van communicatie;

e. inbeslagneming, doorzoeking of vordering van gegevens;
f. oplegging van boetes, sancties of lasten;
g. besluiten die de wet uitdrukkelijk aan de President persoonlijk of aan een minister toekent; of
h. structurele verplichtingen buiten goedgekeurde begrotingskaders.

4. De President kan algemene of bijzondere instructies geven, het mandaat beperken of intrekken en een gemandateerd besluit zelf nemen. Reeds rechtmatig genomen spoedmaatregelen blijven van kracht totdat zij worden gewijzigd of beëindigd.

5. Ieder besluit op grond van dit artikel vermeldt dat het namens de President is genomen door de NC-CSIRT.

Artikel 7

Nationale Cyberveiligheidsraad

1. Er is een Nationale Cyberveiligheidsraad die de President en SUR-CSIRT strategisch, interdepartementaal en beleidsmatig adviseert en coördinatie ondersteunt.

2. De Raad is geen operationeel commandocentrum, opsporingsinstantie of vervanging van het Openbaar Ministerie, het Korps Politie Suriname of enige andere wettelijk bevoegde autoriteit.

3. De Raad bestaat ten minste uit senior vertegenwoordigers en plaatsvervangers van:
   a. SUR-CSIRT,
   b. de met cyberveiligheid en nationale veiligheidscoördinatie belaste afdeling van het Directoraat Nationale Veiligheid (DNV),

c. de met cybercrime en digitale opsporing belaste afdeling van het Korps Politie Suriname,
d. het Openbaar Ministerie voor zover passend binnen diens onafhankelijke wettelijke positie,
e. de met cyberdefensie, militaire informatiebeveiliging of operationele ondersteuning belaste eenheid van het Nationaal Leger, en
f. andere door de President aangewezen vitale sectoren.

4. DNV ondersteunt strategische dreigingsduiding, beleidsintegratie en nationale veiligheidscoördinatie, maar geeft geen dagelijkse operationele leiding aan SUR-CSIRT.

5. De Raad stelt een reglement van orde vast over beveiligde communicatie, vertrouwelijkheid, verslaglegging, belangenconflicten, escalatie en waarneming.

Artikel 8

Melding en informatievoorziening

1. Ministeries, daaronder ressorterende diensten, staatsorganen voor zover zij onder de uitvoerende verantwoordelijkheid van de President vallen, en staatsbedrijven binnen de zeggenschap van de Staat melden een cyberincident of ernstig vermoeden daarvan onverwijld aan SUR-CSIRT, met een eerste kennisgeving uiterlijk binnen 24 uur en een aangevulde rapportage uiterlijk binnen 72 uur, tenzij een kortere termijn uit een andere regeling voortvloeit.

2. Voor constitutioneel onafhankelijke organen, decentrale organen en private beheerders van essentiële of vitale diensten geldt de meldprocedure op basis van de voor hen geldende wet, een convenant, contractuele verplichting of vrijwillige melding. Deze resolutie schept voor hen op zichzelf geen algemene wettelijke meldplicht.

3. Een melding bevat slechts de gegevens die noodzakelijk zijn voor triage, coördinatie en herstel. SUR-CSIRT stelt beveiligde meldkanalen, formulieren, classificatiecriteria en vertrouwelijkheidsregels vast.

4. Meldingen aan SUR-CSIRT vervangen niet de aangifte of melding aan het Openbaar Ministerie, de politie, een toezichthouder of andere wettelijk bevoegde instantie.

Artikel 9

Incidentrespons en tijdelijke technische maatregelen

1. Binnen door de Staat beheerde systemen kan de NC-CSIRT, bij een ernstig of acuut cyberincident, tijdelijke technische responsmaatregelen coördineren of binnen het mandaat gelasten indien deze onmiddellijk noodzakelijk, geschikt, subsidiair en proportioneel zijn.

2. Maatregelen kunnen bestaan uit tijdelijke netwerkisolatie, blokkering van aantoonbaar kwaadaardig verkeer, intrekking van gecompromitteerde accounts of sleutels, tijdelijke beperking van een dienst, veilige verwijdering van malware, herstel uit gecontroleerde back-ups en verscherpte monitoring.

3. Voor systemen buiten de rechtstreekse beheer- of zeggenschapssfeer van de Staat treedt SUR-CSIRT adviserend en coördinerend op, tenzij de beheerder instemt of een uitdrukkelijke wettelijke bevoegdheid bestaat.

4. De maatregel wordt schriftelijk gemotiveerd en gelogd, geldt niet langer dan noodzakelijk, wordt periodiek herbeoordeeld en wordt beëindigd zodra de acute noodzaak vervalt. Bij spoed volgt schriftelijke vastlegging uiterlijk binnen 24 uur.

5. De NC-CSIRT informeert de President onverwijld bij dreigingsniveau 4 of indien een maatregel grote maatschappelijke, economische, diplomatieke of politiek-bestuurlijke gevolgen kan hebben. Deze informatieplicht schorst een onmiddellijk noodzakelijke, rechtmatige maatregel niet.

Artikel 10

Toegang, monitoring en digitale forensiek

1. Structurele technische aansluiting op centrale monitoring vindt uitsluitend plaats op basis van een schriftelijke aansluitovereenkomst, een besluit van de bevoegde beheerder binnen diens wettelijke bevoegdheid of een uitdrukkelijke wettelijke grondslag.

2. De aansluiting wordt beperkt tot vooraf omschreven beveiligingstelemetrie, loggegevens en technische indicatoren. Algemene toegang tot burgerdossiers, inhoud van communicatie, cryptografische sleutels of niet-relevante administratieve gegevens is uitgesloten, behoudens een afzonderlijke wettelijke bevoegdheid en vereiste autorisatie.

3. Toegang tot systemen en gegevens wordt persoonsgebonden geautoriseerd, gelogd, periodiek beoordeeld en beveiligd volgens actuele standaarden. Bewaartermijnen worden vooraf vastgesteld en mogen niet langer zijn dan noodzakelijk.

4. Digitale forensische ondersteuning door SUR-CSIRT is technisch van aard. Indien bewijsvergaring voor strafvordering aan de orde is, wordt gehandeld onder leiding van het Openbaar Ministerie en overeenkomstig de bevoegdheden en chain-of-custody procedures van het Korps Politie Suriname.

5. Onaangekondigde inspecties, verplichte audits, verplichte data-extracties en toegang tegen de wil van de beheerder kunnen niet op deze resolutie worden gebaseerd en vereisen een formele wettelijke grondslag.

Artikel 11

Dreigingsniveaus en escalatie

1. SUR-CSIRT past het volgende bestuurlijke escalatiemodel toe. De NC-CSIRT werkt de technische criteria in een beveiligd protocol uit.

Niveau	Operationele betekenis	Aansturing	President / Raad
1	Beperkte dreiging; reguliere afhandeling.	SUR-CSIRT volgens protocol.	Periodieke rapportage; Raad niet vereist.
2	Verhoogde dreiging of sectorale impact.	NC-CSIRT coördineert.	Versnelde rapportage; Raad op afroep.
3	Ernstig incident met brede of vitale impact.	Nationale respons geactiveerd.	President onverwijld; Raad gedeeltelijk of volledig bijeen.
4	Nationale crisis of dreiging voor staatscontinuïteit.	NC-CSIRT leidt technische coördinatie; bevoegde crisisstructuren worden geactiveerd.	President onverwijld; Raad bijeen; overige wettelijke gezagslijnen blijven intact.

Artikel 12

Geheimhouding, gegevensbescherming en toezicht

1. Eenieder die uit hoofde van deze resolutie toegang heeft tot vertrouwelijke informatie is tot geheimhouding verplicht, behoudens voor zover mededeling bij wet is toegestaan of voor de taakuitoefening noodzakelijk is.

2. Medewerkers en externe deskundigen ondertekenen vóór toegang een geheimhoudings- en integriteitsverklaring en worden passend gescreend. Contractuele geheimhouding vervangt geen wettelijke geheimhoudingsplicht.

3. SUR-CSIRT voert een register van incidenten, besluiten, autorisaties, informatieverstrekkingen en tijdelijke maatregelen en onderwerpt zijn beveiliging en gegevensverwerking periodiek aan onafhankelijke audit binnen de toepasselijke wettelijke kaders.

4. De NC-CSIRT meldt vermoedelijke misbruik, onbevoegde toegang of ernstige tekortkomingen onverwijld aan de President en, indien een strafbaar feit wordt vermoed, aan de bevoegde justitiële autoriteiten.

Artikel 13

Personeel, middelen en financieel beheer

1. Het Kabinet van de President draagt binnen de goedgekeurde begroting zorg voor personele, facilitaire, juridische, inkoop- en financiële ondersteuning van SUR-CSIRT.

2. Benoeming of inzet in vertrouwensfuncties vereist aantoonbare deskundigheid, integriteit, passende veiligheidsscreening, voortdurende opleiding en beschikbaarheid die past bij een 24/7-organisatie.

3. De NC-CSIRT is budgethouder uitsluitend voor zover dit bij afzonderlijk, schriftelijk mandaat en binnen de comptabiliteitsregels is verleend. Inkoop, contractering, subsidie en vermogensbeheer vinden plaats volgens de geldende financiële regelgeving.

4. SUR-CSIRT mag geen vergoedingen heffen of commerciële diensten aanbieden zonder uitdrukkelijke wettelijke of begrotingsrechtelijke grondslag en voorafgaande goedkeuring van de bevoegde autoriteit.

Artikel 14

Overgang naar de Nationale Cybersecurity Autoriteit

1. De in deze resolutie geregelde positionering is tijdelijk en geldt totdat een bij formele wet ingestelde Nationale Cybersecurity Autoriteit operationeel is geworden.

2. De NC-CSIRT bereidt, onder verantwoordelijkheid van de President, de institutionele overgang voor, waaronder een inventarisatie van personeel, budget, activa, contracten, systemen, gegevensverwerkingen, lopende incidenten, internationale relaties en verplichtingen.

3. Overdracht aan de toekomstige autoriteit geschiedt uitsluitend overeenkomstig de instellingswet, uitvoeringsregelingen, begrotingsbesluiten en een door de President goedgekeurd transitieplan, met waarborging van continuïteit, gegevensbeveiliging, archivering, rechtspositie van personeel en lopende onderzoeken.

4. Tot de datum waarop de toekomstige autoriteit feitelijk operationeel is, blijft SUR-CSIRT zijn taken krachtens deze resolutie uitoefenen. De toekomstige wet bepaalt welke taken en bevoegdheden worden overgenomen, gewijzigd of beëindigd.

5. Deze resolutie kan niet worden uitgelegd als vooruitlopen op of vervangen van de formele wet die algemene meld-, toezicht-, audit-, gegevens-, sanctie- of dwangbevoegdheden aan de toekomstige autoriteit toekent.

II. Te bepalen dat:

1. De NC-CSIRT stelt binnen negentig dagen na inwerkingtreding ter goedkeuring van de President ten minste vast:
   a. het incidentclassificatie- en escalatieprotocol;
   b. het informatie-uitwisselings- en vertrouwelijkheidsprotocol;
   c. het protocol digitale forensische ondersteuning en overdracht aan OM/KPS;
   d. het crisiscommunicatieprotocol;
   e. het autorisatie-, logging- en bewaarbeleid; en
   f. het continuïteits- en vervangingsplan.

2. Binnen twaalf maanden na inwerkingtreding en vervolgens jaarlijks wordt de uitvoering geëvalueerd op rechtmatigheid, doelmatigheid, operationele gereedheid, gegevensbescherming, samenwerking en voortgang van de instellingswet.

3. Het Kabinet van de President en de NC-CSIRT zijn, ieder binnen hun taakgebied, belast met de uitvoering van deze resolutie.

4. Deze resolutie en de daarbij behorende bijlage worden bekendgemaakt in het Staatsblad van de Republiek Suriname en treedt in werking met ingang van de dag na haar bekendmaking te rekenen van 01 september 2026.

III. Van deze resolutie afschrift te zenden aan de Vice-President van de Republiek Suriname; de Voorzitter van De Nationale Assemblée; de President van het Hof van Justitie; de Procureur-Generaal bij het Hof van Justitie; de Voorzitter van de Rekenkamer van Suriname; alle Ministers; alle Directeuren van Departementen van Algemeen Bestuur; de Korpschef van het Korps Politie Suriname; de Bevelhebber van het Nationaal Leger; de Chief of Staff van het Kabinet van de President van de Republiek Suriname, de Directeuren van Algemene Zaken en Bestuurlijke en Administratieve Aangelegenheden van het Kabinet van de President van de Republiek Suriname, de Directeur van het Directoraat Nationale Veiligheid; de Directeur E-GOV.

Paramaribo, de 9e september 2026

JENNIFER SIMONS

Uitgegeven te Paramaribo, de 14e september 2026

De Minister van Binnenlandse Zaken,

MARINUS BEE

BIJLAGE behorende bij de resolutie van 09 september 2026, no 1786/RP, houdende instelling en inwerkingtreding van het Suriname Cyber Security Incident Response Team (SUR-CSIRT)

Kritische Infrastructuur

Onder kritische infrastructuur wordt in het bijzonder verstaan:

Digitale infrastructuur & communicatie

Datacentra / cloud providers

Identiteitssystemen

Overheids-ICT

Telecom & internet

Energie & nutsvoorzieningen

Brandstofdistributie

Drinkwater

Elektriciteit

Olie- en gasvoorziening

Financieel systeem

Banken

Betalingsverkeer

Cambio’s

Centrale bank

Verzekeringen

Gezondheidszorg

Farmaceutische distributie

Laboratoria

Ziekenhuizen

Risicovolle industrie (optioneel maar relevant)

Olie- en gasproductie

Chemische / CBRN-sector

Transport & logistiek

Grensposten

Havens

Luchthavens

Luchtverkeersleiding

Veiligheid & hulpdiensten

Brandweer

Crisismanagement

Leger

Nationale veiligheidsdiensten

Openbaar Ministerie

Politie

Voedselvoorziening & essentiële goederen

Agrarische productie

Toeleveringsketens