

Basisprotocol Cyberbeveiliging

De baseline voor cyber security in Suriname opgesteld voor de Surinaamse Bancaire sector

Versie 1.0 – vastgesteld op 17 oktober 2026

Suriname Banking & Finance Summit, Paramaribo, Suriname

©2026 Surinaamse Bankiers Vereniging, All rights reserved

e-mail: secretariaat@sbv.sr

Prins Hendrikstraat 18
Paramaribo-Suriname, S.A.

Totstandkoming

Dit protocol is opgesteld door de Cyber Security Commissie van de Surinaamse Bankiers Vereniging (SBV) in samenwerking met Brightlyn B.V., vertegenwoordigd door de heer S. Gangaram Panday.

Aanleiding

Digitale dreigingen tegen financiële instellingen nemen wereldwijd toe, ook in Suriname. Op dit moment bestaat er geen centraal afgesproken kader voor cyberbeveiliging tussen de Surinaamse financiële instellingen en heeft de Centrale Bank van Suriname vooralsnog geen formele cyberbeveiligingseisen vastgesteld voor de sector.

De Surinaamse Bankiers Vereniging (SBV) neemt hierin het initiatief door, samen met de grootste banken van het land, een eerste gezamenlijk basisprotocol cyberbeveiliging te introduceren. Dit protocol bestaat uit tien basisprincipes en vormt bewust een eenvoudig startpunt: het legt een gemeenschappelijke ondergrens vast waarmee de sector nu al concrete stappen zet en dient als fundament voor verdere, meer gedetailleerde afspraken in de toekomst.

De basisprincipes zijn opgesteld op basis van internationaal erkende referentiekaders. Deze kaders zijn vertaald naar een compacte, praktisch toepasbare vorm die past bij deze eerste stap voor de Surinaamse context.

Doel van dit protocol

Dit protocol legt een gedeelde, minimale basis van cyberbeveiliging vast die voor alle ondertekenende banken geldt, vergroot het onderlinge vertrouwen en de samenwerking in de sector door ervaringen en dreigingsinformatie te delen, en legt een fundament waarop de sector, eventueel in overleg met de Centrale Bank van Suriname, de komende jaren kan doorbouwen naar een volwassener en mogelijk verplichtend kader.

SURINAAMSE BANKIERSVERENIGING
Prins Hendrikstraat 18
Paramaribo-Suriname, S.A.

De tien basisprincipes

De ondertekenende banken onderschrijven de volgende tien basisprincipes als gezamenlijke minimale ondergrens voor cyberbeveiliging.

1. Inventarisatie & risicobeheer

Wij brengen onze kritieke ICT-systemen, data en processen in kaart en beoordelen minimaal jaarlijks welke risico's deze lopen. Deze risicobeoordeling vormt de basis voor onze beveiligingsmaatregelen en investeringsbeslissingen.

2. Toegangsbeveiliging & multifactor-authenticatie

Toegang tot systemen en informatie wordt verleend op basis van het need-to-know- en least-privilege-principe, waarbij gebruikers uitsluitend toegang krijgen tot de systemen, functies en informatie die noodzakelijk zijn voor de uitvoering van hun werkzaamheden. Voor kritieke systemen en beheeraccounts passen wij multifactor-authenticatie (MFA) toe.

3. Patchmanagement & vulnerabilitymanagement

Wij identificeren en beoordelen kwetsbaarheden in onze systemen en verhelpen deze binnen passende termijnen, waarbij kwetsbaarheden met een hoog risico prioriteit krijgen.

4. Betrouwbare back-ups & herstelvermogen

Wij maken regelmatig back-ups van kritieke gegevens en systemen en testen de herstelbaarheid daarvan periodiek. Daarnaast beschikken wij over actuele uitwijk- en herstelplannen, zodat de continuïteit kan worden hersteld binnen vooraf vastgestelde en aanvaardbare termijnen.

5. Beveiligde netwerken en werkplekken

Wij richten netwerken, servers en werkplekken in volgens erkende beveiligingsstandaarden en beschermen deze passend tegen malware, ongeautoriseerde toegang en andere cyberdreigingen.

6. Monitoring & logging

Wij registreren en monitoren relevante gebeurtenissen in kritieke systemen, zodat afwijkend of verdacht gedrag tijdig wordt gedetecteerd, onderzocht en opgevolgd.

SURINAAMSE BANKIERSVERENIGING
Prins Hendrikstraat 18
Paramaribo-Suriname, S.A.

7. Derde-partijrisicomanagement (leveranciers en derden)

Wij beoordelen en beheersen de cyberrisico's van leveranciers en dienstverleners en stellen passende beveiligingseisen vast. De naleving daarvan wordt periodiek gecontroleerd, in het bijzonder wanneer derde partijen toegang hebben tot onze systemen of gegevens.

8. Beveiligingsbewustzijn en cyberhygiëne

Wij bevorderen beveiligingsbewust gedrag door medewerkers periodiek te trainen over cyberrisico's, phishing, veilig handelen en actuele dreigingen, zodat zij beveiligingsincidenten tijdig kunnen herkennen, voorkomen en melden.

9. Incidentmanagement & sectorale samenwerking

Wij beschikken over een actueel en periodiek getest incidentresponsplan. Significante cyberincidenten worden tijdig intern gemeld en, waar van toepassing, gedeeld met de toezichthouder en andere ondertekenende banken, zodat gezamenlijk lessen kunnen worden getrokken en de weerbaarheid van de sector wordt versterkt.

10. Governance, periodieke toetsing en continue verbetering

Wij toetsen periodiek de opzet, werking en effectiviteit van onze beheersmaatregelen, onder meer door middel van interne controles en weerbaarheidstesten. De uitkomsten worden gebruikt om de maatregelen te verbeteren en dit protocol gezamenlijk door te ontwikkelen tot een volwassen, sectorbreed kader.

SURINAAMSE BANKIERSVERENIGING
Prins Hendrikstraat 18
Paramaribo-Suriname, S.A.

Verklaring

Door ondertekening van dit document verklaren de deelnemende banken dat zij de hierboven genoemde tien basisprincipes onderschrijven als gezamenlijke minimale ondergrens voor cyberbeveiliging, zich inspannen om deze principes binnen een redelijke termijn in de eigen organisatie te implementeren of verder te verankeren, relevante ervaringen en inzichten delen om de weerbaarheid van de sector als geheel te vergroten, en zich committeren om dit protocol gezamenlijk, via de Surinaamse Bankiers Vereniging (SBV) en waar mogelijk in overleg met de Centrale Bank van Suriname, verder door te ontwikkelen tot een vollediger en meer verplichtend kader.

Dit protocol is een startpunt en geen eindpunt: het wordt periodiek, bijvoorbeeld jaarlijks, geëvalueerd en waar nodig aangevuld of aangescherpt.

Ondertekening

Originele versie ondertekend door een bestuurslid van elk van de onderstaande banken op 17 oktober 2026 tijdens de Suriname Banking & Finance Summit.

Het protocol is gedeeld met de Centrale Bank van Suriname. De toezichthouder heeft de volgende reactie gegeven:

> *"De Centrale Bank van Suriname heeft kennisgenomen van het Cyber Security Protocol dat door de Surinaamse Bankiersvereniging is opgesteld om de sector handvatten te bieden voor de praktische implementatie van basismaatregelen op het gebied van cybersecurity. Hoewel de Centrale Bank geen inhoudelijke bijdrage heeft geleverd aan de totstandkoming van dit protocol, onderschrijft zij het belang van sectorinitiatieven die bijdragen aan het vergroten van de algehele cyberweerbaarheid. De ontwikkeling van dergelijke kaders sluit aan bij eerdere oproepen van de Centrale Bank om binnen de sector samen te werken en – indien gewenst – gezamenlijk normen te ontwikkelen die hieraan bijdragen."*

Prins Hendrikstraat 18
Paramaribo-Suriname, S.A.

Bronnen

- Nationaal Cyber Security Centrum (NCSC) - Zorgplicht Cyberbeveiligingswet (NIS2): ncsc.nl
- Nationaal Cyber Security Centrum (NCSC) - Incidentrespons: waar begin ik?: ncsc.nl
- Cyber Security Raad (CSR): Handreiking Cybersecurity voor Bestuurders en Bedrijfseigenaren, tabel met voorbeelden van Key Control Indicatoren: cybersecurityraad.nl (PDF)

SURINAAMSE BANKIERSVERENIGING
Prins Hendrikstraat 18
Paramaribo-Suriname, S.A.