

Draft version 0.1b

Schiphol Group: **Security Catch-22** structure versus **"Safeguard"** method
 Just a few example observations, focused on 3 telltale subjects.

Examples picked from a very long list of blatant security and compliance issues highlighting the overall **conundrum** in 6 areas of security management within High-Risk Vital Infrastructure context.



Royal Schiphol Group is een luchthavenonderneming met een belangrijke maatschappelijke opdracht. Royal Schiphol Group is eigenaar en exploitant van Amsterdam Airport Schiphol, Rotterdam The Hague Airport en Lelystad Airport en heeft een meerderheidsbelang in Eindhoven Airport. De luchthavens van de groep creëren waarde voor de samenleving en de economie, met veiligheid als essentiële factor. Alle Nederlandse luchthavens van de



		Impact →				
		Negligible	Minor	Moderate	Significant	Severe
↑ Likelihood	Very Likely	Low	Moderate	High	High	High
	Likely	Low	Moderate	Moderate	High	High
	Possible	Low	Low	Moderate	Moderate	High
	Unlikely	Low	Low	Moderate	Moderate	Moderate
	Very Unlikely	Low	Low	Low	Moderate	Moderate

Schiphol

Beveiligingsmaatregelen Schiphol

Schiphol wil een veilige omgeving zijn voor iedereen. Met verschillende beveiligingsmaatregelen proberen we aanslagen op onze luchthaven en de vliegtuigen te voorkomen.

Securitygebieden

De luchthaven is bijvoorbeeld ingedeeld in verschillende securitygebieden. In deze verschillende securitygebieden worden diverse beveiligingsniveaus gehanteerd. Elk niveau kent een aantal specifieke beveiligingsmaatregelen die in zwaarte kunnen toenemen.

De toegang tot de verschillende gebieden van de luchthaven is in veel gevallen beperkt tot alleen diegenen die een geldige reden hebben om zich daar te begeven en over een geldig toegangsbewijs beschikken. Dit geldt niet alleen voor personen, maar ook voor voertuigen.

Securitycontroles

Voor dat men toegang krijgt tot een securitygebied worden alle personen, waaronder passagiers, personeel en iedereen die voor zijn of haar werkzaamheden op Schiphol komt, gecontroleerd. Dit gebeurt voordat men daadwerkelijk toegang krijgt tot het desbetreffende gebied. Hiermee houden we zicht op wie zich met welke motivatie in de verschillende securitygebieden bevindt.

De securitycontroles op Schiphol richten zich op het vaststellen of een persoon (en voertuig) geautoriseerd is om in een bepaald gebied te komen (de toegangscategorie), en afhankelijk van het beveiligingsniveau worden de personen, de meegebrachte voorwerpen en voertuigen ook gecontroleerd op de aanwezigheid van verboden voorwerpen (het beveiligingsonderzoek). Denk maar aan de verschillende controles als je op reis gaat als passagier.

Betrokken partijen

Schiphol vindt een veilige omgeving belangrijk, maar de beveiligingsmaatregelen zijn ook verplicht gesteld door de Nederlandse én internationale overheden. Deze controleren regelmatig of de beveiligingsmaatregelen op Schiphol op orde zijn. Daarnaast zijn er diverse organisaties op verschillende manieren betrokken bij de veiligheid van en op de luchthaven, zoals de AIVD, NCTV, Koninklijke Marechaussee en meerdere beveiligingsbedrijven.

...ETC..

Pas op met wat je deelt op social media

Natuurlijk mag je trots zijn dat je werkt op Schiphol. Maar, pas op met wat je deelt op insta, facebook, LinkedIn of andere social media. Deel bijvoorbeeld géén foto's van je toegangspas voor de luchthaven, werkschema's of gevoelige informatie over je werkplek. Zet ook op LinkedIn geen uitgebreide informatie je werkzaamheden. Criminelen zitten namelijk ook op social media. En dan kunnen ze je makkelijk vinden. Kijk hier hoe ze dat doen.

Deel geen details over je werk met anderen

Criminelen herken je niet zomaar. Vaak zijn ze vriendelijk en goedgebekt. Ook weten ze hoe ze mensen moeten bespelen. Wees dus voorzichtig!

www.schiphol.nl/en/schiphol-group/management-royal-schiphol-group/

- Learning :(# Publishing & Leaking large quantities of sensitive "inside" information, 24/7 to public internet,) ..thus to unauthorized people => incl. hostile actors.. Via: documents (digital & physical), photo / video, social media, network protocol layers, out-sourced systems, unfiltered meta-data, work chats in public area's, etc...
- Learning :(# Ignoring mandatory essential risk management rules & regulations, shifting responsibility to 'others', + false positive status statements in reports.



Hedzer Komduur 1st
 Director Safety and Environment and CISO at Royal Schiphol Group
 The Randstad, Netherlands · [Contact Info](#)
 500+ connections

About
 I am driven, like assessing the big picture, but also have a keen eye for details, both in business and in people.

Experience

Royal Schiphol Group
 Full-time · 7 yrs 9 mos

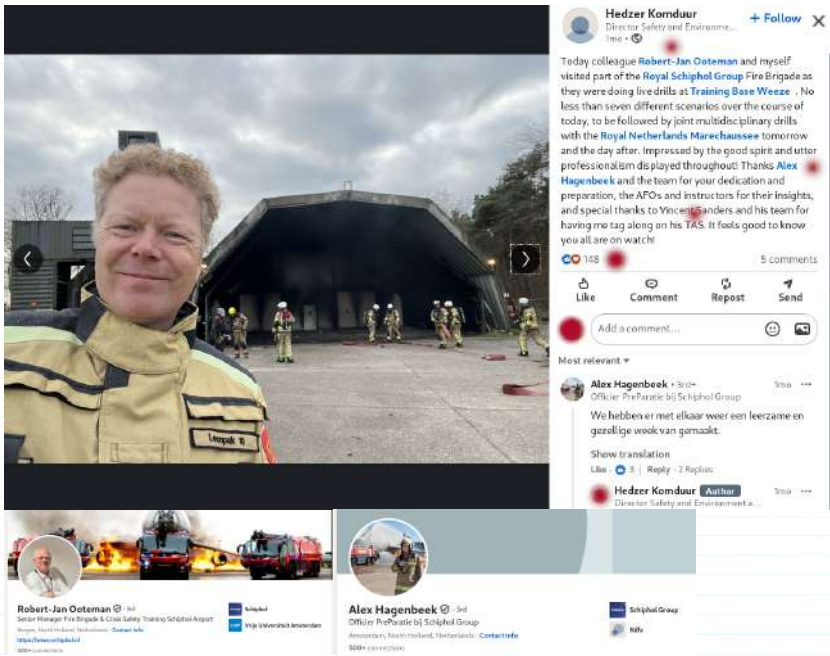
- Director Safety and Environment and CISO**
 Oct 2022 - Present · 2 yrs 4 mos
 Schiphol, North Holland, Netherlands
 Safety Manager Schiphol Airport
 Responsible for HSE Office, Airport Fire Brigade, Crisis & Safety Training and the European Entry/Exit (EES) program
 Chair of Information Security Board
 Stakeholder management on a local, national and international level
 Representative of Schiphol in Regional Policy Team of the Safety Region Kennemerland in case of crises, disasters and disruptions of public order pertaining to the airport
 Leadership, Airport Management and +7 skills
- Acting Director Safety, Security and Environment**
 Sep 2022 - Oct 2022 · 2 mos
 Responsible for Security Policy, 24/7 Security Operations, Corporate Investigations, HSE Office, Airport Fire Brigade, Crisis & Safety Training and the European Entry/Exit (EES) program
 Stakeholder management on a local, national and international level
 Representative of Schiphol in Regional Policy Team of the Safety Region Kennemerland in case of crises, disasters and disruptions of public order pertaining to the airport
 Leadership, Airport Management and +7 skills
- Deputy Director Safety, Security and Environment**
 Jun 2020 - Sep 2022 · 2 yrs 4 mos
 Schiphol, North Holland, Netherlands
 Responsible for Security Policy, 24/7 Security Operations, Corporate Investigations, Airport Fire Brigade and Crisis & Safety Training

TNO Prins Maurits Laboratory

Hedzer Komduur, M.Sc.
 Research Scientist
 Rocket Technology



"It's like we face reality, my friends... We're not exactly rocket scientists."



Director Safety & Environment

Hedzer Komduur



Luchthavens vind ik machtig interessant; het zijn plekken waar elke dag tienduizenden mensen bij elkaar komen. Om te reizen naar familie, vrienden, of voor zaken. Dagelijks spannen duizenden mensen zich in om al die reizigers van dienst te zijn. Iedereen die je op Schiphol ziet heeft zijn eigen, unieke verhaal. Ik zorg er samen met mijn team voor dat al die mensen elke dag veilig kunnen reizen en werken op Schiphol, en we onze overlast richting de omgeving zoveel mogelijk beperken. Zaken als de energietransitie vragen ook op veiligheidsgebied de nodige inspanningen, dus geen dag is hetzelfde. Voor mijn werk heb ik zelf vaak via Schiphol gevlogen en ben ik op hele bijzondere plekken geweest. Ik kijk er naar uit om onze dochter kennis te laten maken met een van mijn favoriete steden ter wereld: New York. Hier liggen voor mijn vrouw en mijzelf mooie herinneringen, die we graag met haar willen delen.

```
* images.ctfassets.net/biom0eqy16b/6W4gp9ayaJGZRY773MAGqB/d01a85a5fa63d620a1ff2340617fd7c/hedzer_komduur.jpg
X-Cache: Miss from CloudFront
X-Amz-CF-POP: AMS5-P2
Server: Contentful Images API
Access-Control-Allow-Origin: *
ETag: "1cc5c434858863b48090718ad57c923c"
Last-Modified: Thu, 27 Oct 2022 12:13:57 GMT
...

Return-Path: <Hedzer.Komduur@schiphol.nl>
Received: from [40.107.21.44] (EUR05-VI1-obe.outbound.protection.outlook.com) with Microsoft Exchange Server
v15.20.8230.016*
X-MS-Exchange-CrossTenant-id: 27776982-d882-41b2-95ac-322f28d5a2ce
X-MS-Exchange-Organization-AuthSource: XVCQREdUWTRc4XdcqZQx==
X-MS-Exchange-CrossTenant-mailboxtype: HOSTED
x-ms-PublicTrafficType: Email
Disposition: automatic-action/MDN-sent-automatically; displayed
```

```
Di, 9 Dec 2024 10:08:00 AM
"Hedzer Komduur" <Hedzer.Komduur@schiphol.nl> wrote:

> Geachte heer/mevrouw,

> Onderstaande e-mail ontving ik via collega Odette Rudolf. Als CISO voor de Luchthaven Amsterdam Schiphol verneem ik graag welke acties wij in uw ogen zouden moeten nemen. Tevens wijst ik u op de mogelijkheid van het doen van een Responsible Disclosure via https://www.schiphol.nl/nl/pagina/responsible-disclosure-melding/

> Met vriendelijke groet,

> Hedzer Komduur

> -----Original Message-----
> From: Odette Rudolf <Odette.Rudolf@schiphol.nl>
> Sent: Monday, 9 December 2024 10:08
> To: Komduur, Hedzer <Hedzer.Komduur@schiphol.nl>
> Subject: FW: uitnodiging gesprek
> Importance: High

Hi Hedzer

Zoals zojuist besproken onderstaand email van Anna

mvg

Odette Rudolf
Bedrijfsrechercheur P&S
```

To: [Odette Rudolf](#) (@odetterudolf)
 Subject: Re: verzoek contact
 Date: Wed, 20 Nov 2024 10:02:00

Zou jij deze 2 vragen perlijk beantwoord willen krijgen binnen de organisatie ?

Waarom worden er IT systemen gebruikt voor verwerking van vertrouwelijke operationele gegevens waarvan men weet dat die niet echt voldoen aan de voorschriften en geen functioneel IPS hebben?

Waarom deelt Schiphol Group (zonder expliciete toestemming van personen) hoeveelheden vertrouwelijke informatie over medewerkers, partners, klanten en bezoekers met 13+ beruchte Amerikaanse bedrijven? Zonder enige "nodzaak", in overtreding van AVG/GDPR, 9e Art.18 en eigen beleid documenten. Maakt 't ook voor hostile actors eenvoudiger om aan ID diefstal en Social Engineering, Chantage/Deception/Beïnvloeding te kunnen doen, toch?

* schiphol.nl/en/page/data-processing-badge-center/
 * customer.bookingbug.com/?cliënt=schiphol
 * ovesta.schiphol.nl/ovesta/prod/inloggegevensvergeten
 * etc.

On Tue, 19 Nov 2024 10:31:28 +0000
 "Odette" <Odette.Rudolf@schiphol.nl> wrote:
 > Beste Anna
 >
 > Zou je contact met mij op willen nemen?



Instagram



odetterudolf Follow ...

41 posts 377 followers 491 following

Odette Rudolf
 @odetterudolf

On Wed, 20 Nov 2024 10:02:00
 "Odette" <Odette.Rudolf@schiphol.nl> wrote:
 > Beste Anna?
 >
 > Leuke foto heb je bijgevoegd! Al voelt het een beetje ongepast

Dat "ongepast" gevoel is dus een van de kernpunten.. (spiegelde aan de wand :-)
 omdat opvallend veel "security" functionarissen binnen en rond de Schiphol Airport organisatie zichzelf en de rest roekeloos Extra kwetsbaar maken door o.a. "ongepast" delen van allerlei informatie over zaken waar ook kwaadwillenden gratis gebruik van maken om
 Te veel beveiliging functionarissen hebben blijkbaar (nog) niet de nodige "awareness" van welke verregaande negatieve gevolgen er zijn van o.a. dergelijke "social media" publicaties en niet-versleutelde email conversaties, gebruik van ms-sharepoint-cloud, etc.. (negezen van de essentiële "Need to know" regel) !! tot dat ..ieder voor zich eens flink op de snufferd gaat en 't aan eigen lijve ondervind wat er aan covert activiteiten gaande achter de schermen.
 Iemand had er bijvoorbeeld ook voor moeten zorgen dat de email systemen geen leesbevestiging naar buiten sturen (maarja o.a. de Schiphol CISO mist 't droodnodige aan motivatie om 't werk echt wegelij te doen, blijkst..). En ook jij had er basis weet & awareness van moeten hebben, wat de gevolgen zijn als informatie lekkages voorkomen, ..door nalatigheid van C-Level management.

't is daardoor deels ook de reden met de kran open met de jip & janneke bureauszaten 'verbeter projecten' :-)
 ?? (((H.. men kint nu alnog om wel goed functionerende basis awareness training te gaan regelen voor alle beveiliging mensen. Zoals a.a. Mic en Mossad en "... garelateerde functionarissen die krijgen om überhaupt "security" taken naar behoren uit te kunnen voeren zonder brokken te maken.)
 Zo lang mensen zoals jij als "Bedrijfsrechercheur RSG - Afdeling Bedrijfsbeveiliging" ..eenduidig onvoldoende awareness en context kennis training krijgen, blijf je een easy target voor pro's die fratsen willen uithalen via de Schiphol Airport infrastructuur, natuurlijk !! (Security & Compliance maturity level ?)

Nog een tip:
 Overschrijf zelf je "social media" publicaties met wat semi willkeurige plaatjes en teksten die helemaal niets met jou te maken hebben, incl een profiel foto van een actrice of stripfiguur ofzo. Mis ook facebook en andere soorten commentaren bij posts van nogal specifieke functionarissen in sleutelposities bij andere high-risk organisaties...
 ? - Tenzij; je maar al te graag t.z.t. eens zelf flink de pionier wil zijn wat betreft ID diefstal, Chantage, APT's op personal devices, enz. . enz..





Author : Dijkstra, Björn
 Creator : Microsoft® Word 2016
 Create Date : 2020/08/07 15:00:57+02:00

Schiphol

Aanvraagformulier Special Operations op Schiphol

Dit formulier is bedoeld voor het aanvragen van een speciaal verzoek (special operations) op Schiphol. Onder special operations verstaan we een gepland en georganiseerd verzoek, bijeenkomst of activiteit met zichtbare impact op Schiphol en haar bedrijfsvoering.

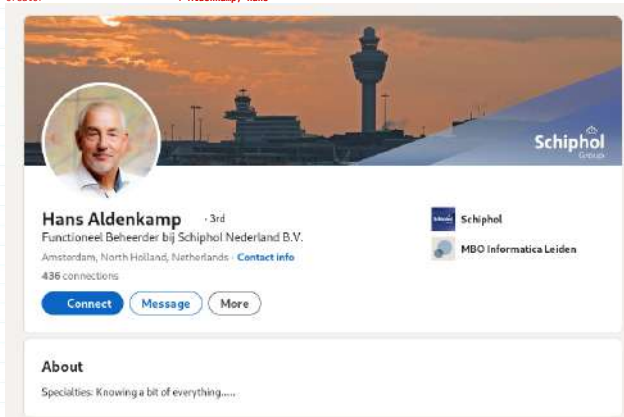
Onderwerp*
 Omschrijf kort het onderwerp van je aanvraag.

Voor-enachternaam*

Organisatie*

Telefoonnummer*
 Wil hieronder je contactgegevens in, zodat we je kunnen bereiken.

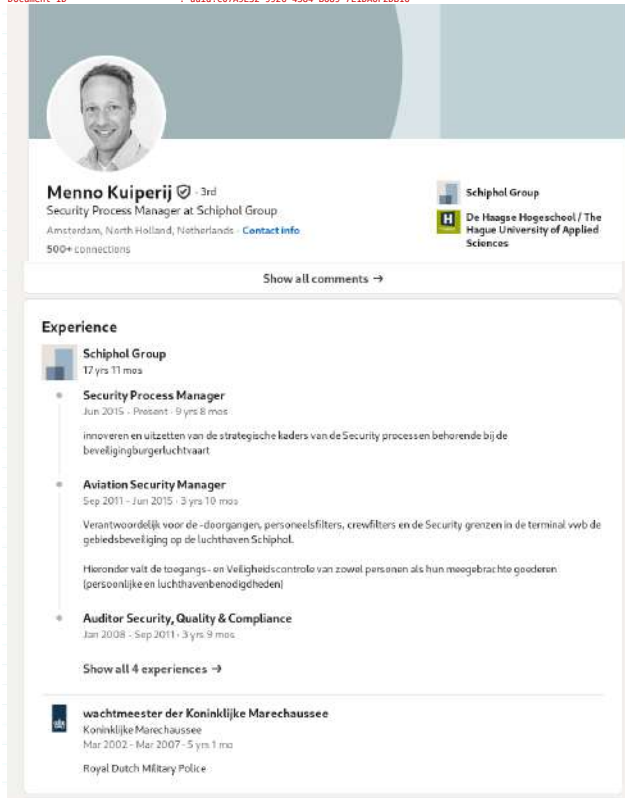
* 2.2.1_Werkinstructie_Manager_planner.pdf
 Create Date : 2024-03-04 08:28:10+01:00
 MSIP Label 5237ac-88-813e-467d-90ba-6ce-279e-3edc-8 Name: 5237ac88-813e-467d-90ba-6ce279e3edc8
 MSIP Label 5237ac-88-813e-467d-90ba-6ce-279e-3edc-8 Set Date: 2022-08-24T10:00:37Z
 MSIP Label 5237ac-88-813e-467d-90ba-6ce-279e-3edc-8 Size: 161: 27776982-6882-41b2-95ac-322f28d5a2ce
 Document ID : uuid:e16c36a1-60ea-4548-a631-fc63c467d584
 Instance ID : uuid:b428f508-7774-49f7-9dbb-c7ffd79fce34
 Creator : Aldenkamp, Hans



Ervaring

- Schiphol**
 25 jaar 5 maanden
 - Functioneel Beheerder LMS**
 mrt. 2021 - heden · 3 jaar 11 maanden
 Schiphol
 - Manager Safety Training Center (VTC) Schiphol**
 mrt. 2016 - mrt. 2021 · 5 jaar 1 maand
 Amsterdam Area, Netherlands
 Het Veiligheidstrainingcentrum (VTC) Schiphol is al decennia hét trainingscentrum als het om de veiligheid op Schiphol gaat. Wij beschikken over een uitstekend en ervaren team van trainers maar ook de laatste trainingsmiddelen. Veel mensen kennen het VTC Schiphol vanwege zijn bijzondere brandweeroefenplaats.
 - Information Security Advisor**
 sep. 2007 - mrt. 2016 · 8 jaar 7 maanden
 Amsterdam Area, Netherlands
 Providing the organization with Information Security (IS) advices when needed; develop Information Security policies; setting up and maintaining a governance structure for IS; Chairman of the tactical Information Security taskforce at Schiphol.
 - Operations Manager**
 sep. 1999 - sep. 2007 · 8 jaar 1 maand
 Performed special Operations within the Passenger Operations Department. Involved

* Acces_Policy_2025__ENG_-_pdf
Product : Microsoft Word voor Microsoft 365
MSIP Label 5237ac-88-813e-467d-90ba-6ce-279e-3edc-8 Site Id: 27776982-d882-41b2-95ac-322f28d5a2ce
Creator : Kuiperij, Menno
Creator Tool : Microsoft Word voor Microsoft 365
Create Date : 2024-12-17 12:19:39+01:00
Document ID : uid: C07A9E32-9926-4384-B689-7E1DA6F2D816



Menno Kuiperij · 3rd
Security Process Manager at Schiphol Group
Amsterdam, North Holland, Netherlands · [Contact info](#)
500+ connections

[Show all comments](#) →

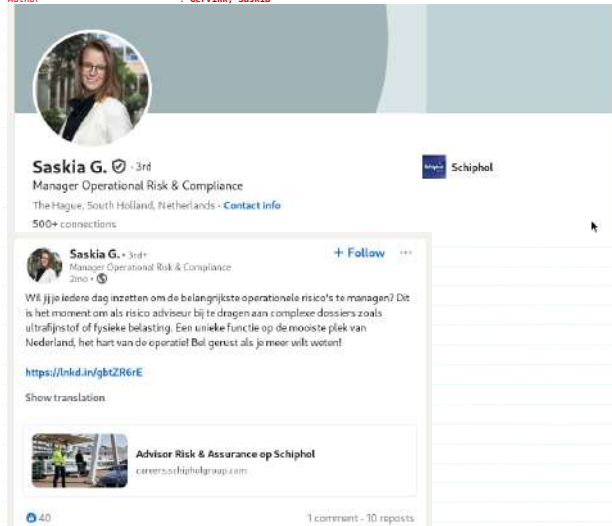
Experience

- Schiphol Group**
17 yrs 11 mos
- Security Process Manager**
Jun 2015 - Present · 9 yrs 8 mos
Innoveren en uitzetten van de strategische leiders van de Security processen behorende bij de bereijnging burgerluchtvaart
- Aviation Security Manager**
Sep 2011 - Jun 2015 · 3 yrs 10 mos
Verantwoordelijk voor de -doorgangen, personeelsfilters, crewfilters en de Security grenzen in de terminal vwb de gebiedsbeveiliging op de luchthaven Schiphol.
Hieronder valt de toegang- en Veiligheidscontrole van zowel personen als hun meegebrachte goederen (persoonlijke luchthavenbenodigdheden)
- Auditor Security, Quality & Compliance**
Jan 2008 - Sep 2011 · 3 yrs 9 mos

[Show all 4 experiences](#) →

- wachtmeester der Koninklijke Marechaussee**
Koninklijke Marechaussee
Mar 2002 - Mar 2007 · 5 yrs 1 mo
Royal Dutch Military Police

* License_to_Operate_for_Ground_Handlers_Version_Final_Setting_23_October_2023.pdf
Creator Tool : Microsoft Word for Microsoft 365
Create Date : 2023-10-25 17:52:09+02:00
Document ID : uid: 12A312F9-390E-4500-9830-8C9C202CA181
MSIP Label 5237ac-88-813e-467d-90ba-6ce-279e-3edc-8 Site Id: 27776982-d882-41b2-95ac-322f28d5a2ce
Author : Gervink, Saskia



Saskia G. · 3rd
Manager Operational Risk & Compliance
The Hague, South Holland, Netherlands · [Contact info](#)
500+ connections

Saskia G. · 3rd
Manager Operational Risk & Compliance
2mo · [+ Follow](#)

Wt jijje ledere dag inzetten om de belangrijkste operationele risico's te managen? Dit is het moment om als risico adviseur bij te dragen aan complexe dossiers zoals ultrafijnstof of fysieke belasting. Een unieke functie op de mooiste plek van Nederland, het hart van de eportatie! Ben gerust als je meer wilt weten!

<https://lnkd.in/gbZR6rE>

[Show translation](#)

Advisor Risk & Assurance op Schiphol
careers.schipholgroup.com

40 · 1 comment · 10 reposts

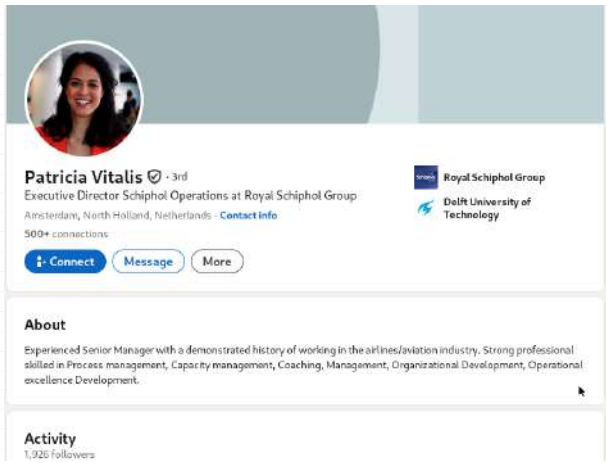
* Safety_Security_0_A_2024_-_EN.pdf
* Safety_Security_instruction_employees.pdf
...



Sander Hengeveld · 3rd
Senior Brandmanager bij Royal Schiphol Group
Bloemendaal, North Holland, Netherlands · [Contact info](#)
500+ connections

Schiphol
Universiteit van Amsterdam

COO



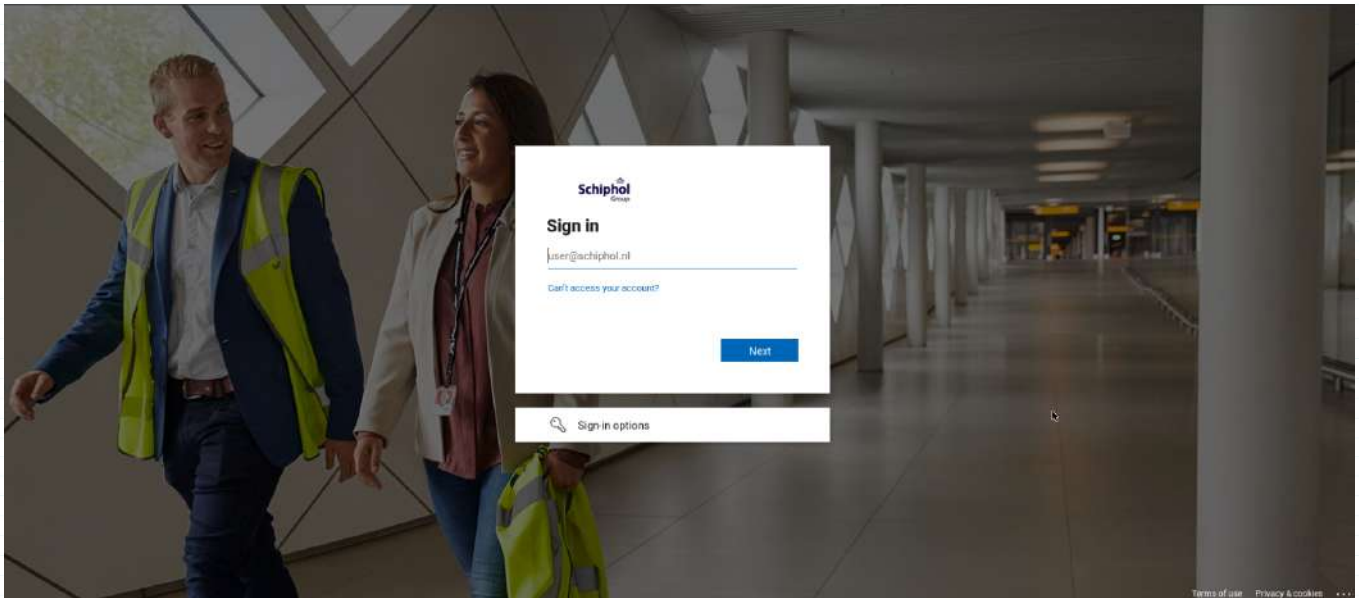
Patricia Vitalis · 3rd
 Executive Director Schiphol Operations at Royal Schiphol Group
 Amsterdam, North Holland, Netherlands · [Contact info](#)
 500+ connections

[Connect](#) [Message](#) [More](#)

About
 Experienced Senior Manager with a demonstrated history of working in the airlines/aviation industry. Strong professional skilled in Process management, Capacity management, Coaching, Management, Organizational Development, Operational excellence Development.

Activity
 1,920 followers

- # Remote (covert) Access is "allowed", to Vital Infra and operational elements.
- # Admin rights access from unknown sources is also "allowed" (by CISO & Co), without any need to expose those powerful functions to unknown/unauthorized outsiders all over the world (incl. China, Russia, USA, etc.)
- # No functional IPS/IDS possible, due to lacking 'security' architecture.
- # No functional detection of (large quantities) of Classified information extraction.
- # [classified info]
- # [classified info]



Schiphol Developer Center


API & Solutions How it works Examples Sign in Sign up More

Important notice
 For security purposes, your IP address will be logged when making API requests starting 2024-07-15.

Forgot password
 Please enter the email address you used to sign up to this site. Instructions on how to reset your password will be sent to you.

Email address *

[Send instructions](#) [Sign in](#)

Sign in to Schiphol Maps (acceptatie 11.3) 

Schiphol

ArcGIS login

Keep me signed in

[Sign in](#) [Cancel](#)

[Forgot password?](#)

Home
Welcome to My Schiphol

Forgot Your Password?

Enter your email address and we will send you the instructions to reset your password.

Email address*

Send

[Back to login screen](#)

Schiphol Group

Get back into your account

verification step 1 > verification step 2 > choose a new password

Please choose the first contact method we should use for verification:

- Text my mobile phone
- Approve a notification on my authenticator app
- Enter a code from my authenticator app
- Approve the notification we're sending to your app by entering the number shown below.
- 56**

[Cancel](#)

Status	Method	Domain	File
200	GET	cdn.auth0.com	main.com.mim.css
200	GET	cdn.auth0.com	auth0-iron-owlight.svg
200	GET	cdn.schiphol.nl	index_De_VEw1.js
200	GET	cdn.schiphol.nl	index_Cb0actfyp.css
200	GET	cdn.schiphol.nl	fonticom.svg
200	GET	cdn.schiphol.nl	route_Fu1lgsxwU2
302	GET	login.schiphol.nl	ctiphschicater
200	GET	login.schiphol.nl	schipholstate

Schiphol

Home
Welcome to My Schiphol



You've got mail!


Open your inbox, as an email is waiting for you with instructions on how to reset your password.

[Resend email](#)

Vulnerabilities by impact types

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2015	0	0	0	0	0
2016	2	0	0	2	0
2017	3	0	0	4	3
2018	0	0	0	1	1
2019	2	1	3	0	1
2020	10	3	7	8	2
2021	5	4	6	5	1
2022	2	1	5	3	2
2023	3	0	2	0	0
2024	1	1	7	4	0
Total	28	10	30	27	10

You have reported an error page. The error message is: [Error message] If you are still having the problem, please contact us.




THE NEW EXPERIENCE IN THE BEST TO QUALITY AND SERVICE

IAS is a leading provider of ground handling services at Amsterdam Schiphol Airport. We provide a comprehensive range of services including aircraft cleaning, catering, baggage handling, and more. Our services are designed to ensure the highest standards of safety and efficiency for all flights.

At IAS, we are committed to providing the best possible service to our clients. We have a team of experienced professionals who are dedicated to ensuring that every flight is handled with care and precision.

The best of services that have not been met in order to handle their cargo handling and other important details of the flight process. Backed by leading edge infrastructure, we provide highly efficient and reliable services to our clients.





Sign in with your organizational account

...../.....

.....

[Sign In](#)

Reception can be reached at +31203995321

Ivory Tower: Lack of wanting to be "in control" of security and compliance = risk-management ?



Lennert l'Amie (1985) is als senior manager bij Schiphol verantwoordelijk voor zo'n beetje alle digitale processen van de luchthaven. Hij stuurt een team met 150 IT-professionals aan, en dit altijd met een glimlach.

'Ik doe alleen dingen waar ik energie van krijg. Dat klinkt wellicht egotistisch, maar het maakt dat ik altijd met enthousiasme door kan en dat reflecteert op mijn omgeving.' Respect voor anderen vindt l'Amie echter even belangrijk als eigenschap. 'Wie je ook bent, wat je ook doet, je draagt altijd bij aan de successen van het bedrijf.'

Uitdagingen de rode draad

Complexe situaties en uitdagingen lopen al vanaf het begin als een rode draad door de carrière van volledige operations. In 2015 lonkt een heel andere operatie: die van Schiphol. l'Amie start bij Schiphol Telematics, om in 2019 verder te groeien bij Schiphol Group tot senior manager business platform operations

Leiders cruciaal voor groei

'Goede (op)leiders zijn cruciaal in mijn groei geweest. De keuze voor een functie is minder relevant. Ik kies voor de manager die me uitdaagt, die me iets kan leren en die me ruimte geeft om mezelf te ontwikkelen en te falen. Dat heeft me elke keer geholpen om een vervolgstap te zetten, waarbij zij wellicht al veel eerder zagen dat dat moment zou komen.'

Wat de toekomst betreft, zal volgens l'Amie het onderscheidend vermogen van bedrijven bepaald worden door de snelheid van het kunnen reageren op verandering. 'Nieuwe leiders omarmen verandering als een constante. Ze blijven inspireren en een diverse en inclusieve cultuur creëren.'

Schiphol kleedt Schiphol Telematics uit

18 december 2019



18 november 2019

Een groot deel van de taken van Schiphol Telematics, onderdeel van Schiphol Group, wordt uitbesteed aan Conscia, Allinq en Securelink. Van de telecomoperator voor de luchthaven blijft een regieorganisatie over. Een deel van de medewerkers kan bij Schiphol Telematics blijven werken.

Schiphol Telematics (ST) is zo'n twintig jaar de telecomoperator op en rond de luchthaven Schiphol. Het bedrijf levert diensten op het gebied van IP-netwerken, internet, vaste en mobiele netwerken en internet-of-things.

Wanneer de Conscia, Allinq en Securelink de taken van ST in handen nemen, zal ST meer technologische en innovatieve kennis zitten om goed in te kunnen blijven spelen op relevante ontwikkelingen en klantbehoeften op de luchthaven.

Na vier, zes of acht jaar wordt 'uitbesteed' in de markt voor het outsourcing van de beveiliging van kritische infrastructuur. Deze drie bedrijven geselecteerd: Conscia, Allinq en Securelink. De looptijd van de contracten is vijf jaar. Over de laatste van de vier contracten worden geen details bekend gemaakt.

De beveiligingsintegrator Securelink, tegenwoordig onderdeel van de Franse netwerkdiensverlener Orange, krijgt de verantwoordelijkheid voor de beveiliging van Dataconnectiviteit en communicatieoplossingen.



#

```
inetnum:      89.248.140.184 - 89.248.140.111
netname:      AAS-NL
descr:        A. A. S. T/ICT
country:      NL
admin-c:      ED679-RIPE
tech-c:       ED679-RIPE
status:       ASSIGNED PA
mnt-by:       MNT-STNET
created:      2015-12-11T10:56:54Z
last-modified: 2015-12-11T10:56:54Z
source:       RIPE

person:       Eddy Dobma
address:      Schiphol
phone:        +31(0)610339753
nic-hdl:      ED679-RIPE
mnt-by:       MNT-STNET
created:      2008-12-09T12:12:19Z
last-modified: 2021-06-08T13:11:40Z
source:       RIPE
```

% Information related to '89.248.128.0/20AS42517'

https://77.241.235.132/ [SiteManager 1130 Mobile broadband]



Digi Connect ME4 Configuration and Management

Login [Help](#)

Welcome to the Configuration and Management Interface of the Digi Connect ME4.

Please specify the username and password to login to the web interface.

See the User Guide and documentation for more information on logging in or retrieving a lost password.

Username:

Password:

Copyright © 1994-2010 Digi International Inc. All rights reserved.
www.digi.com

PROFLEET Login Home | Logout | Help

Password change

Identification:

Old password:

New password:

New password confirmation:

Quick start guide display

mSafe Product | Prijzen | Over Ons | Contact [Start Gratis](#)

Veilig bestanden versturen

Met mSafe verstuur je eenvoudig en volledig **AVG-compliant** vertrouwelijke bestanden. Of je nu werkt in de gezondheidszorg, juridische sector, het onderwijs of een andere branche, met één klik verstuur je **jeuw gegevens veilig**. Maak je geen zorgen meer over databreken – binnen 30 seconden verzend je je eerste bestand veilig.

[Start nu](#) Waarom mSafe

KVK **EGON** **Schiphol** **Rabobank**

Taal: Nederlands

Schiphol **mSafe**

Veilig traceerbaar & controleerbaar bestanden delen

E-mailadres:

Wachtwoord:

Onthoud mijn e-mailadres

[Wachtwoord vergeten?](#)
[Problemen met inloggen?](#)

Door in te loggen ga je akkoord met onderstaande voorwaarden: [Waarvoor?](#)
[Privacyverklaring](#)
[EULA](#)

mSafe

Gebruikersnaam of e-mailadres:

Wachtwoord:

Onthoud mij

Je wachtwoord vergeten? [Ga naar mSafe](#)

[Privacyverklaring](#)

Nederlands | Wijzig

User(s) Identified:

```

>| admin
>| hennie_fn8338in
>| thijs569v31
>| 33 vulnerabilities identified;

```

Vulnerabilities by Impact Type

Year	Critical	High	Medium	Low	Information Leak
2015	0	0	0	0	1
2016	1	0	0	0	1
2017	0	1	1	1	1
2018	1	0	0	0	1
2019	1	0	0	0	0
2020	1	1	1	1	0
2021	1	0	0	0	0
2022	0	2	2	2	0
2023	0	0	0	0	1
2024	0	2	0	0	0
Total	6	7	5	5	6

This page lists vulnerability statistics for all versions of WordPress. Vulnerability statistics provide a quick overview.

Not secure 89.248

TechPoint

User name:

Password:

[Download help PDF \(English \(Denmark\)\)](#)

TechPoint v3.002.016, © TechSolutions AS, [www.techpoint.no](#) - all rights reserved.

PREFACE 3
 Other guidelines 4
 HISTORY 4
 GENERAL 4

TechPoint's default factory user is "root" and password "ITechsolutions"



Instellingen

TechPoint root | log out

System Toegang Gebruikers Log/Report Behouden

- Area set
- Area set
- Area set

Events (3131)

Level	Event	Tijd	Verwijderd
Info	Web login	2017-10-24 13:00:18	
Alarm	SIA Transmission error	2017-10-24 13:00:18	<input checked="" type="checkbox"/>
Info	LAN Link restored	2017-10-24 13:00:18	
Alarm	LAN Link lost	2017-10-24 13:00:18	<input checked="" type="checkbox"/>
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	GPI Informatie	2017-10-24 13:00:18	
Info	GPI Informatie	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	GPI Informatie	2017-10-24 13:00:18	
Info	GPI Informatie	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	
Info	SIA Intrusion Event	2017-10-24 13:00:18	

Event details

Level: Info
 Event: GPI informatie
 Tijd: 2017-10-24 13:00:18
 ID: 12345

Details

Naam	Waarde
Thor	GPI-PC
Informatie	CPI connector established 45.227.254.49

Geolocation data from IPGeolocation.io Product: API, real-time

IP ADDRESS: 45.227.254.49 ISP: XWIN UNIVERSAL LTD
 COUNTRY: Lithuania ORGANIZATION: Flyservers S.A.
 REGION: Vilniaus Apskrėtis LATITUDE: 54.69062
 CITY: Vilnius LONGITUDE: 25.26960

Geolocation data from IPRegistry.co Product: API, real-time

IP ADDRESS: 89.248.140.109 ISP: Schiphol Telematics B.V.
 COUNTRY: Netherlands ORGANIZATION: A.A.S. TACT (st.nl)
 REGION: Flevoland LATITUDE: 52.39127
 CITY: Almere Stad LONGITUDE: 5.23801

< Home System instellingen Configuratie Monitor

< Toegang

Toeganginstellingen

Instellingen

Card credentials ververs Opslaan

Algemeen

Cardless access Disabled

Cardless access as text

Data modem Monitor

Verwijder ververs

Type	Waarde	Signal quality	Network status	Received	Transmitted	Last error
Network Online	NL KPN KPN	33%		336520	282232	

RS 485 |
 IO |
 Smart Intego (TCP-IP) |
 Data modem |
 Integratie |
 SIA Alarm transmitter

SIA Alarm transmitter Monitor

Verwijder | ververs

Account	Transmit count	Transmit failures	Primary line	Backup line 1	Backup line 2	Backup line 3
			G4S Online	G4S Online	N/A	N/A

Database Structure | Browse Data | Edit Pragma's | Execute SQL

Table: Event_LogDetails

ID	EVENT LINK	TYPE LINK	TABLE ID	OWNER ID	VALUE
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard afgesloten 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard afgesloten 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard afgesloten 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard afgesloten 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard afgesloten 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard afgesloten 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard afgesloten 89.248.140.109
2500			6000		1 GPI-PC
504			504		ThorGuard aansluiting gelukt 89.248.140.109
2500			6000		1 GPI-PC



29 februari
Tap&go met je Digital Travel Credential!



Met het oog op privacy

Zoals u mag verwachten, valde Schiphol aan alle wettelijke eisen voor privacy. Wij doen er dus alles aan om uw persoonlijke gegevens veilig te houden.

De biometrische informatie is versleuteld opgeslagen in een beveiligde database of op de chip van uw Privilium kaart. In ons Privacystatement leggen we wegbereid om hoe we met uw gegevens omgaan.

Remote access, Infra layout and Vulnerability detection
... is **allowed** by CISO & IT Manager & COO & CEO :(

```

Host: 185.138.242.12  nginx 1.25.5
Host: 185.138.242.13  nginx 1.25.5
Host: 189.69.228.86  Microsoft IIS httpd 10.0
Host: 189.69.228.44  [Remote-Web-Access]
Host: 189.69.225.52  [Remote-Web-Access]
Host: 189.69.231.220  ZyxEL ZyWALL http config
Host: 189.69.228.93  Microsoft IIS httpd 10.0
Host: 189.69.224.156  [Remote-Web-Access]
Host: 189.69.228.84  [Remote-Web-Access]
Host: 189.69.224.188  [Remote-Web-Access]
Host: 189.69.228.106  [Remote-Web-Access]
Host: 189.69.228.84  Microsoft IIS httpd 10.0
Host: 189.69.225.205  [Remote-Web-Access]
Host: 189.69.224.45  Mongose httpd
Host: 189.69.228.45  [Remote-Web-Access]
Host: 77.241.235.116  [Remote-Web-Access]
Host: 77.241.233.132  [Remote-Web-Access]
Host: 77.241.237.84  [Remote-Web-Access]
Host: 77.241.234.52  [Remote-Web-Access]
Host: 77.241.227.132  DrayTek Vigor ADSL router httpd
Host: 77.241.238.172  DrayTek Vigor ADSL router httpd
Host: 77.241.233.7  Microsoft HTTPAPI httpd 2.0 (SSDP)
DPM)
Host: 77.241.227.148  FRITZ!Box http config
Host: 77.241.231.4  [Remote-Web-Access]
Host: 77.241.228.116  [Remote-Web-Access]
Host: 77.241.225.116  [Remote-Web-Access]
Host: 77.241.232.154  [Remote-Web-Access]
Host: 77.241.232.152  [Remote-Web-Access]
Host: 77.241.234.28  [Remote-Web-Access]
Host: 77.241.232.153  [Remote-Web-Access]
Host: 77.241.225.252  Lighttpd
Host: 77.241.238.132  DrayTek Vigor ADSL router httpd
Host: 77.241.225.228  [Remote-Web-Access]
Host: 77.241.225.236  FRITZ!Box http config
Host: 77.241.225.188  Mongose httpd
Host: 77.241.224.188  [Remote-Web-Access]
Host: 77.241.223.124  [Remote-Web-Access]
Host: 77.241.236.132  DrayTek Vigor ADSL router httpd
..ETC..

Host: 77.241.233.164  [Remote-Web-Access]
Host: 77.241.232.159  [Remote-Web-Access]
Host: 77.241.232.149  [Remote-Web-Access]
Host: 77.241.230.140  [Remote-Web-Access]
Host: 77.241.238.140  [Remote-Web-Access] Server
Host: 77.241.227.28  FRITZ!Box http config
Host: 77.241.235.132  Apache httpd
Host: 77.241.238.92  DrayTek Vigor ADSL router httpd
Host: 77.241.232.212  DrayTek Vigor ADSL router httpd
Host: 77.241.229.148  [Remote-Web-Access]
Host: 77.241.229.148  [Remote-Web-Access]
Host: 77.241.227.28  [Remote-Web-Access]
Host: 77.241.232.140  [Remote-Web-Access]
Host: 77.241.229.12  [Remote-Web-Access]
Host: 77.241.236.140  [Remote-Web-Access]
Host: 77.241.233.18  [Remote-Web-Access]
Host: 77.241.225.108  [Remote-Web-Access]
Host: 77.241.234.204  [Remote-Web-Access]
Host: 77.241.229.156  Big5-Connect-ME4 *****
Host: 77.241.238.68  [Remote-Web-Access]
Host: 77.241.224.188  DrayTek Vigor ADSL router httpd
Host: 77.241.232.153  [Remote-Web-Access]
Host: 77.241.238.76  DrayTek Vigor ADSL router httpd
Host: 77.241.238.264  [Remote-Web-Access]
Host: 77.241.232.147  [Remote-Web-Access]
Host: 77.241.224.124  Apache httpd
Host: 77.241.238.84  DrayTek Vigor ADSL router httpd
Host: 77.241.227.208  FRITZ!Box http config
Host: 77.241.233.36  [Remote-Web-Access]
Host: 77.241.233.11  Apache httpd
Host: 77.241.238.188  DrayTek Vigor ADSL router httpd
Host: 77.241.231.228  DrayTek Vigor ADSL router httpd
Host: 77.241.229.148  [Remote-Admin-Access] DrayTek Vigor ADSL router sshd 2.0 (protocol
2.0)
Host: 77.241.231.156  [Remote-Admin-Access] OpenSSH 8.4p1 Debian 5deb11a3 (protocol 2.0)
Host: 77.241.225.92  [Remote-Admin-Access] (protocol 2.0)
Host: 77.241.235.116  [Remote-Admin-Access] OpenSSH 8.5 (protocol 2.0)
Host: 89.248.149.244  [Remote-Admin-Access] OpenSSH 7.4p1 Debian 19deb0b7 (protocol 2.0)
Host: 89.248.133.212  [Remote-Admin-Access] OpenSSH 5.4p1 Debian 6 (protocol 2.0)
Host: 89.248.139.125  [Remote-Admin-Access] Dropbear sshd 2019.78 (protocol 2.0)
Host: 89.248.131.212  [Remote-Admin-Access] DrayTek Vigor ADSL router sshd 2.0 (protocol
2.0)
..ETC..

```

P.R. Propaganda, ==> Creating a "False sense of Security"



[About](#) - [Services](#) - [Partners](#) - [News](#) - [Events](#) - [F](#)

Home > News > News > Schiphol Airport Most Cyber-Secure Airport in the World

Schiphol Airport ~~Most Cyber-Secure~~ Airport in the World

04 Feb 2020 | Author: HSD Foundation

The 2020 annual meeting of the World Economic Forum (WEF) urged the consideration of emerging cybersecurity challenges in the aviation industry, as addressed in its "Advancing Cyber Resilience in Aviation: An Industry Analysis" report. To shed some light on the current state of aviation transportation security, ImmunWeb decided to conduct research on cybersecurity, compliance and privacy of some of the world's largest airports.

Top 3 Most Secure Airports

During the research 3 international airports were identified that successfully passed all the tests without a single major issue being detected:

1. Amsterdam Airport Schiphol (EU/ The Netherlands)
2. Helsinki-Vantaa Airport (EU)
3. Dublin Airport (EU)

Read more about the state of Cybersecurity at Top 100 Global Airports, [here](#).

www.schiphol.nl/en/work-at-schiphol/golden-rules-of-safety/

Golden Rules of Safety

The Golden Rules of Safety stem from the main risks involved in working at our airport. They are important tools which will help you to work safely. You must therefore make sure that you are familiar with them and apply them at all times and in all places. Safety is a shared responsibility, so remind each other of the rules and tackle your colleagues about any unsafe behaviour. All under our motto: safety first.

Challenge

Challenge →

Last Minute Risk Analysis

Last Minute Risk Analysis →

Remind other people of the rules

Working safely starts with you, but don't keep it to yourself. Help other people and keep each other alert. Take a critical look at your own performance, be open to feedback and draw people's attention to any unsafe behaviour. And don't forget to give compliments too!

Golden Rule 1: I speak out about unsafe working practices

- Take immediate action in the event of an unsafe situation.
- Take responsibility for your own safety and that of others.
- Address colleagues about unsafe or irresponsible behaviour.
- Report unsafe situations immediately so that colleagues can learn from them.
- Discuss safety dilemmas with your manager.
- Accept it when colleagues speak to you about unsafe behaviour.

Downloads: Safety for everyone

Onveilig gedrag bespreekbaar maken

Veel incidenten zijn het gevolg van onveilige gedragingen.

Schiphol wil het bespreekbaar maken van onveilig gedrag stimuleren om ongevallen te voorkomen.

The Schiphol logo, consisting of the word "Schiphol" in white text on a red rectangular background.

One moment please

we are checking that your connection to Schiphol.nl is secure.

Waiting for www.schiphol.nl to respond...



<https://www.schiphol.nl/en/disclaimer/>

Disclaimer website

The use of our website

1. No Guarantees

This website and the information provided on it, are offered as is and as available. Although Schiphol Nederland B.V. (SNBV) does its utmost to include accurate and complete information on this website, SNBV gives no explicit or implied guarantee of its completeness and accuracy, therefore no rights can be derived from the prices mentioned and products shown on this website. No rights can be derived from the current waiting times shown on the website and in the app. Nor does SNBV guarantee that this website will be available without interruption or delay.

2. No Liability

In visiting this website you agree that SNBV is not liable for any direct or indirect loss resulting from the use of this website or the information on it. Likewise, SNBV accepts no liability for the services offered by third parties via this website.

3. Links

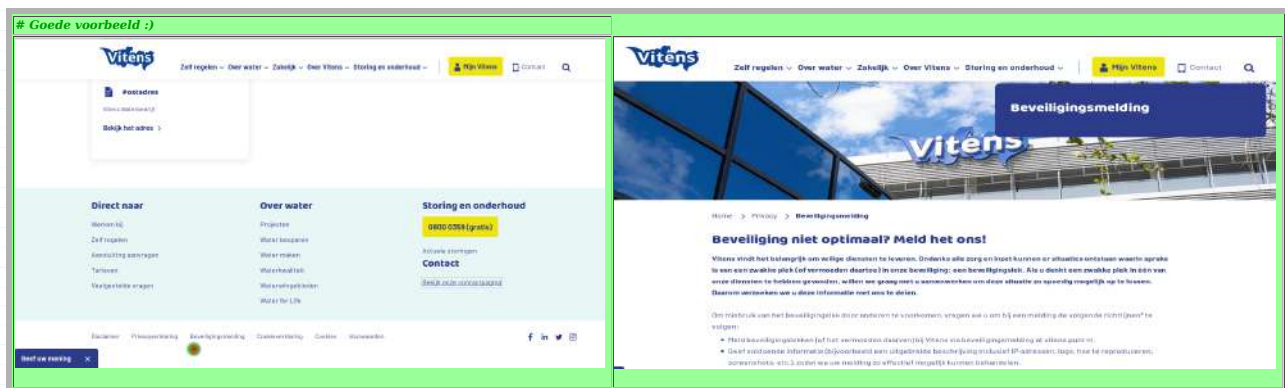
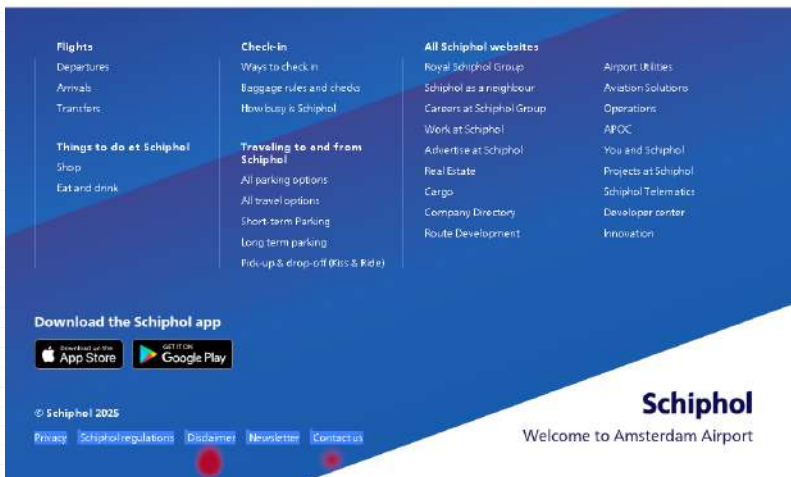
This website can contain links or referrals to third-party websites over which SNBV has no authority or control. SNBV is not responsible or liable for the content of such third-party websites or the links that they may contain.

4. Intellectual Property Rights

All intellectual property rights relating to the information on this website, including but not limited to the materials, pictures, illustrations, names, logos, brands and other distinguishing marks belong to SNBV or other Schiphol Group companies or possible licensors. The availability of this information implies no licence for the reproduction and/or distribution of this information. Such actions are not permitted without prior written consent from SNBV or the relevant third party except in the case of legally permissible actions such as printing or downloading information in this website for personal, non-commercial use. It is not allowed to frame this site.

5. Responsible Disclosure notification

We want all legal entities belonging to the Royal Schiphol Group to be legally established in the Netherlands to protect online as well as possible. Have you discovered a weak spot in our IT systems? We would like to hear this from a [Responsible Disclosure notification](#). This helps you to make our digital environment more secure. Thanks in advance for your help!



What to do if you find a vulnerability in our system

If you find a vulnerability in our IT system we would like you to tell us about it immediately, so that we can take whatever measures are necessary to solve the problem as quickly as possible. **We take all notifications of security issues in our IT systems very seriously.** To be able to respond to these notifications responsibly, we would like to make the following agreements with you. Have you found a problem, and you are wondering how it should be reported? We would like to hear about it immediately, in the following way.

- Email your findings as quickly as possible to responsible [full stop] disclosure [at] schiphol [full stop] nl. If possible, encrypt this email using Schiphol's [PGP key](#); this will prevent your information from falling into the wrong hands.
- In the email explain how you encountered this issue, so that we can reproduce it. Describe the problem and provide the relevant IP address or URL.
- Include your own contact details, such as an email address or telephone number. We can then get in touch with you to work together on a secure solution.
- We will respond as quickly as possible to report on ongoing progress.

<https://www.schiphol.nl/en/page/responsible-disclosure-notification>

Deliberately creating a narrow scope, to avoid 'hearing' about sec issues which by law have to be reported and resolved :(

If you discover a flaw in or breach in the IT systems of one or more of Royal Schiphol Group's legal entities that has its registered office in the Netherlands, then please let us know. It is important that we take every possible measure and precaution to give ourselves the best digital protection available. For that reason, we ask you to handle digital security responsibly and that you carefully study the rules for [Responsible Disclosure notifications](#). Thanks in advance for your cooperation.

What can be reported

Please let us know if you encounter problems with our digital systems, such as:

- Remote Code Execution
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Injection vulnerabilities
- Broken authentication and session management.
- Encryption-related flaws
- Unauthorized access to data
- APIs that are insufficiently protected

Exceptions

Before reporting a vulnerability, make sure to check if it is not listed in the exceptions:

[Exceptions Responsible Disclosure \(0.1 MB pdf\)](#)

Wrong Exclusions lists, showing that there is an Ivory Tower ostrich-politics structure within C-level management & "security" dept.

Responsible Disclosure Exceptions

Application

- Self-XSS that cannot be used to exploit other users
- Verbose messages/files/directory listings without disclosing any sensitive information
- CORS misconfiguration on non sensitive endpoints
- Missing cookie flags on non sensitive cookies
- Missing security headers which do not present an immediate security vulnerability
- Missing DNS entries
- Cross-site Request Forgery with no or low impact
- Presence of autocomplete attribute on web forms.
- Reverse tabnabbing
- Bypassing rate-limits or the non-existence of rate-limits.
- Best practices violations (password complexity, expiration, re-use, etc.)
- Clickjacking on pages without sensitive actions
- CSV Injection
- Sessions not being invalidated (logout, enabling 2FA, ..)
- Hyperlink injection/takeovers
- Mixed content type issues
- Cross-domain referer leakage
- Anything related to email spoofing, SPF, DMARC or DKIM
- Username / email enumeration
- E-mail bombing
- HTTP Request smuggling without any proven impact
- Homograph attacks
- XMLRPC enabled
- Banner grabbing /version disclosure
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Weak SSL configurations and SSL/TLS scan reports
- Not stripping metadata of images
- public API keys without proven impact

General

- In case that a reported vulnerability was already known to the company from their own tests, it will be flagged as a duplicate.
- Theoretical security issues with no realistic exploit scenario(s) or attack surfaces, or issues that would require complex end user interactions to be exploited, may be excluded or be lowered in severity
- Spam, social engineering and physical intrusion
- DoS/DDoS attacks or brute force attacks.
- Vulnerabilities that are limited to non-current browsers (older than 3 versions) will not be accepted
- Attacks requiring the usage of shared computers, man in the middle or compromised user accounts
- Recently disclosed zero-day vulnerabilities in commercial products where no patch or a recent patch (< 2 weeks) is available. We need time to patch our systems just like everyone else - please give us 2 weeks before reporting these types of issues.
- Attacks requiring unrealistic user interaction

Author : **Jong, Rob de**
Creator : Microsoft® Word 2016
Create Date : 2020-08-03 10:03:34+02:00



LinkedIn profile of Rob de Jong. The profile includes a circular profile picture, the name 'Rob de Jong', and location 'Leusden, Utrecht, Nederland'. It also lists affiliations with 'Schiphol' and 'SANS Technology Institute', and mentions '917 volgers' and 'Meer dan 500 connecties'. The 'Info' section lists specialties: 'Incident Handling, Blue Teaming, Security Operations Center (SOC), CSIRT...'. There is a 'meer weergeven' link at the bottom.

Harsh self-Contradictions and false promises, in legal and security statements :(

Wat mag je van ons verwachten?

- Indien je bij de melding van een door jouw geconstateerde kwetsbaarheid in een ICT-systeem van Schiphol aan bovenstaande voorwaarden voldoet, zal Schiphol geen juridische consequenties verbinden aan deze melding.
- Schiphol behandelt een melding vertrouwelijk en deelt persoonlijke gegevens niet zonder toestemming van de melder met derden, tenzij dit juridisch verplicht is.
- We sturen je binnen vijf werkdagen een ontvangstbevestiging.
- Op korte termijn kan je een reactie op een melding verwachten. Hierin vermelden we de beoordeling van de melding en een verwachte datum voor een oplossing.
- We houden je op de hoogte van de voortgang in het oplossen van het probleem.
- Schiphol lost het door jou geconstateerde beveiligingsprobleem zo snel mogelijk op. We streven ernaar om dit binnen 90 dagen te doen. Na de oplossing kunnen we in overleg bepalen of en op welke wijze we over het probleem extern communiceren.

<!=>

Be careful not to break the law

Please take great care when looking into the security of our IT systems, as you may accidentally break Dutch or international laws. This may open you up to possible criminal charges. The rule of law supersedes the rules set out by Amsterdam Airport Schiphol, so take great care to ensure you are not engaging in any illegal activities that we are required to report to the authorities.

Royal Schiphol Group Responsible Disclosure Hall of Fame

- De disclosure moet opgelost zijn vóór het plaatsen van je naam en details. Dit betekent dat je naam niet geplaatst wordt zolang Schiphol er voor kiest om het (nog) niet op te lossen.
- De melding wordt automatisch van de hall of fame gehaald na twee jaar.

Op onze Responsible Disclosure Hall of Fame kunnen wij plaatsen:

- Jouw voornaam, achternaam en/of pseudoniem (naar jouw keuze)
- **Omschrijving van de gevonden kwetsbaarheden**
- Aantal van gevonden kwetsbaarheden per melder

Royal Schiphol Group would like to thank the following people for their contribution to keeping Schiphol Group's information provision secure.

[View the 2025 Responsible Disclosure Hall of Fame](#)

Who	Number of notifications
-----	-------------------------

[View the 2024 Responsible Disclosure Hall of Fame](#)

Who	Number of notifications
-----	-------------------------

Arif Nawaz Minhas	1
-----------------------------------	---

Martin van Wingerden	1
--------------------------------------	---

Kasper Karlsson	1
---------------------------------	---

Hassan Muhammad	1
---------------------------------	---

Latest update: 8 August 2024

ST did buy a ISO27001 certificate from corrupt auditor, illegally, without actual compliance.

10. Security and confidentiality

- 10.1. As a result of the ISO norm 27001:2005 that ST possesses, ST must comply with strict regulations with respect to security and information security. Within this framework, ST has the right to set additional criteria for the contracting party with respect to security and confidentiality. These additional criteria may concern accessibility, and an additional agreement may be required, for example with respect to co-locations and/or access.
- 10.2. ST ensures the security of service(s) and/or equipment as far as possible.
- 10.3. ST complies with the legal requirements concerning the security of registrations and personal data wherever this may be applicable.
- 10.4. ST is obliged to take sufficient measures to protect the confidentiality of all data vis-a-vis third parties, in whatever form, within the framework of this agreement, where ST knew (or should have known) that this was confidential. This is guaranteed within the ST organisation.

General terms and conditions of trading 5



INTERNET

Betrouwbaar, snel internet voor al uw zakelijke behoeften

Een snelle, betrouwbare internetverbinding is de levensader van veel bedrijfsprocessen. Die rol zal in de nabije toekomst alleen maar groter worden. ST biedt internetverbindingen die aan de hoogste eisen voldoen en de digitalisering van de luchthaven en iedereen die er werkt mogelijk maken. Onze unieke en betaalbare maatwerkoplossingen, bewezen expertise, beveiliging en 24/7-service maken van ST een betrouwbare partner.



Schiphol group & ST: "Security" => Kastje => Kastje => Muur => Zwart gat..
responsible.disclosure@schiphol.nl ; access@schiphol.nl ; badgecenter@schiphol.nl ;
Evasion of taking responsibilities.

* Example α

- 1) Security issues report send to: responsible.disclosure@schiphol.nl
- 2) Takes 4 days before anyone responds (outsourced to external BV with jnr's instead of pr's..?)
- 3) Ask for irrelevant extra info, blindly follow written procedure without understanding the context.
- 4) Don't handle it, but say they will forward it on, to ST IT Dept.
- 5) Nothing further happens... no response, no update, no fix, nothing..

Thank you for your recent contact with our team. We have been working on your responsible disclosure issue. As promised, we would like to update you as to the progress of the request. Schiphol CSIRT handles the responsible disclosures of Schiphol Group. In this case, it concerns an IP address provided by the ISP service of Schiphol Telematics to an external customer, which falls outside the Schiphol CSIRT mandate. However, we have contacted Schiphol Telematics to inform them about this security issue at one of their customers. Best regards, Schiphol CSIRT Responsible_disclosure@schiphol.nl

==> !? Misleading statements by Schiphol Group.

- Op korte termijn kan je een reactie op een melding verwachten. Hierin vermelden we de beoordeling van de melding en een verwachte datum voor een oplossing.
- We houden je op de hoogte van de voortgang in het oplossen van het probleem.
- Schiphol lost het door jou geconstateerde beveiligingsprobleem zo snel mogelijk op. We streven

* Example β

Automatisch antwoord: Schiphol access pas verloren



* Example Δ

X-Originatororg: schiphol.nl
X-MS-Exchange-Crosstenant-Authas: Internal
X-MS-Exchange-Crosstenant-Authsource: V11PR04MB3055.eurprd04.prod.outlook.com
X-MS-Exchange-Crosstenant-Id: 27776982-d882-41b2-95ac-322f28d5a2ce
X-MS-Exchange-Crosstenant-Mailboxtype: HOSTED

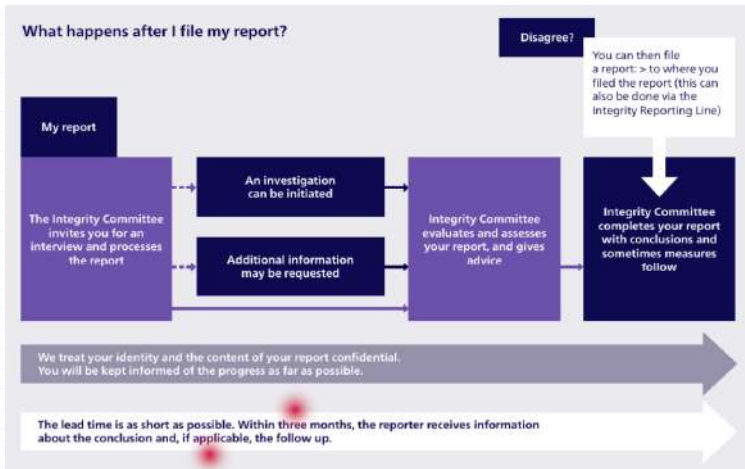
Not read: Schiphol access card verloren

From: Badgecenter
Onderwerp: Schiphol access card verloren
Verzonden: Vrijdag 1 november 2024 (UTC+01:00) Amsterdam

is verwijderd op donderdag 7 november 2024 08:08 UTC+01:00 Amsterdam

message/disposition-notification

Final-recipient: RFC822; Badgecenter@schiphol.nl
Disposition: automatic-action/MDN-sent-automatically; deleted
X-MSEch-Correlation-Key: xml6BSh5hEagfdX+xroizQ==
Original-Message-ID:
X-Display-Name: Badgecenter



!# Project is **not** even compliant with Wbni, BIO, AVG/GDPR, ISO27001, NIS2, etc..

#-----!----->> **Remote system access and modification by unauthorized entities is allowed.** *Even from China, Russia, USA, etc..

[classified info] *

[classified info] Kmar;MinBZK/MinJenV;NCTV

[classified info] IL&T / RDI

Geef criminelen geen kans

Welkom op sterkeluchthaven.nl. Hier vind je alles om jezelf, je collega's en de luchthaven Schiphol te beschermen tegen de invloed van criminelen. Doe de interactieve e-learning of bekijk handige tips. Heb je iets vreemds gezien? Meld dat dan. Er zijn allerlei mogelijkheden. En weet, je bent nooit alleen. Wij geven criminelen geen kans.

[Bekijk de video](#)

Oog in Oog met Ondernijning

In deze serie maken we kennis met mensen die van dichtbij hebben meegemaakt hoe criminelen te werk gaan op luchthaven Schiphol en wat daarvan de gevolgen zijn.

[Back to Live Site](#)

Webflow
Log in to manage your site.

Email:
Password:
Forgot it? [Link](#)

[Log in](#)



Over ons

Samenwerken aan misstanden op de luchthaven Schiphol

De georganiseerde criminaliteit probeert de luchthaven Schiphol en de mensen die daar werken, te misbruiken voor bijvoorbeeld diefstal en smokkel. Daarom werken Belastingdienst, Douane, FIOD, gemeente Haarlemmermeer, Koninklijke Marechaussee, Openbaar Ministerie, Politie, RIEC Noord-Holland, KLM en Schiphol Group al lange tijd samen om ondermijnende criminaliteit en misstanden op luchthaven Schiphol aan te pakken. Ook andere bedrijven zijn onderdeel van de aanpak door barrières tegen criminaliteit op te werpen. Samen houden we de luchthaven sterk. Naar aanleiding van de rapportage "Ondermijning op en rond luchthaven Schiphol" is de urgentie bekrachtigd en de aanpak verder geïntensiveerd.

AANMELDEN BEDRIJVEN

Meer informatie

Om ons gesprek met u goed voor te kunnen bereiden, vragen wij u om nog wat extra informatie over uw bedrijf door te geven:

Werkzaamheden van uw bedrijf:

Geef uw beste beschrijving van uw werkzaamheden met het bedrijf

Lid van uw bedrijf en/of luchthaven Schiphol:

Geef uw beste beschrijving van uw lidmaatschap op Schiphol aan

Volgende >

Tijds

Medewerkers van uw bedrijf voeren werkzaamheden uit op:

- Landbouw
- Aardolie
- Beeld
- Open van bedrijf

Volgende >

Tijds

Aantal medewerkers op Schiphol:

Waarvan met een Schipholpas:

Waarvan met een andere toegangspas:

Volgende >

Tijds

Wat uw bedrijf doet om ondermijning te voorkomen is:

Volgende >

Meer informatie

Om ons gesprek met u goed voor te kunnen bereiden, vragen wij u om nog wat extra informatie over uw bedrijf door te geven:

Bedankt!

We nemen zo snel mogelijk contact met u op.



LESMATERIAAL
TIPS
MELDEN
VERHALEN

Over ons
Prijzen
Veelgestelde vragen
Privacy statement

DE Medius
Linxor

Samen werken aan een veilige en integrale luchthaven



2 Schiphol's security areas

Introduction

Amsterdam Airport Schiphol makes every effort to ensure a secure environment for everyone. Both passengers and staff are screened at various points in the airport. Take, for example, the security checkpoint at the staff entrance in the terminal. This check is intended to make sure that you are not carrying any dangerous items with you. Everyone of any age, male and female, security staff and airline captains alike must pass through this security checkpoint. In addition, security staff also screen all goods that you want to take with you, such as hand baggage, hold baggage and tools.

All of these security measures are necessary at Schiphol in view of the various attacks on airports and aircraft in the past. Schiphol has put a comprehensive set of security measures in place to prevent the possibility of such an attack.

Measures to ensure a secure environment are not only important to Amsterdam Airport Schiphol, they are



compulsory under Dutch and international law, and regular checks are carried out to ensure that Schiphol fulfils its obligations.

Security areas

Amsterdam Airport Schiphol is divided into the following security areas:

Security areas
Airside Security Restricted Area - Critical Parts
Airside Non-Security Restricted Area's
Airside Demarcated Area's
Landside Secured Premises by A.A.S.

These security areas are described in Chapter 5 of the 'Toegangsbeleid beschermde en bedrijfsbeveiligde gebieden Amsterdam Airport Schiphol (Access Policy A.A.S.)'.

I

11

3 Schiphol's passes and tests

Types of passes

Schiphol uses a variety of passes for people and vehicles to give access to Airside Security Restricted Area - Critical Parts, Airside Non-Security Restricted Areas, Airside Demarcated Areas and /or Landside Secured Premises by A.A.S.

The number of people who have access to these areas is kept to a minimum. Schiphol Passes are provided only to people in regular employment at the airport and who meet legal requirements as well as Schiphol's own requirements. The colour and letter codes on a pass indicate the areas it gives you access to, as set out in brief in the table below.



Colour / letter	Area
Green	Access to the passenger areas in the terminal
Blue	Access to airside perimeter roads
Orange	Access to the passenger areas in the terminal and airside perimeter roads
Grey	Access to Schiphol-East business park
Black background on pass	Access to Schiphol-East business park
Letter B on the pass	Access to the baggage areas
Letter P on the pass	Access to the aprons

Schiphol Passes are also available for visitors. Passes for visitors do not have a photograph. Visitors, like staff members, must wear their pass so that it is clearly visible at all times, and must always be accompanied by a Schiphol Pass holder authorised to accompany visitors. The Schiphol Pass holder is personally responsible for the visitor.

Types of tests

One of the conditions that needs to be met to qualify for a Schiphol Pass providing access to a security-restricted area is the successful completion of a safety and security test. When applying for a pass for the first time, you will

12

13

5 Rules for use of the Schiphol Pass

Rules for use of Schiphol Pass

The Schiphol Pass is a strictly personal access pass. Only the pass holder is entitled to the rights granted by his or her respective pass. The pass holder is the person whose name is stated on the pass itself. The following rules apply to the use of your Schiphol Pass:

- Always display your Schiphol Pass clearly when in the Airside Security Restricted Area - Critical Parts, Airside Non-Security Restricted Areas, Airside Demarcated Areas or Landside Secured Premises by A.A.S. and ensure that others do too.
- Never lend your Schiphol Pass to anyone else.
- Never allow someone to tag along with you on your Schiphol Pass. For instance, do not let people through a door or into a lift.
- Do not use the Schiphol Pass outside working hours or for personal ends. For instance, you are prohibited from using the pass to wave off or collect friends or family from a gate.

Correct Schiphol Pass

Employers are responsible for ensuring that employees have a Schiphol Pass for the areas in which they carry out their work.

Misuse of Schiphol Pass

Misuse of a Schiphol Pass can be grounds for the pass being immediately confiscated or blocked without further justification from the airport operator.

Reporting a lost Schiphol Pass

If you lose your Schiphol Pass you must report this immediately to the Badge Center on +31 (0)20 6012626 during office hours, or to the Security Control Center on +31 (0)20 6013000 outside of office hours.



20

21



If only, this section 6 would actually be properly enforced by C-Level & CISO (+Kmar & MinBZK)
 # But it clearly is not :(

6 Enforcement and sanctions

Need for enforcement

Without Safety & Security rules, it is likely that dangerous situations would soon arise. These rules will unfortunately be broken at times, which is why Amsterdam Airport Schiphol has established enforcement measures and sanctions related to the Safety & Security rules.

Supervision

Security staff and officials appointed by Amsterdam Airport Schiphol provide supervision at the airport to ensure that rules are adhered to. These individuals can stop you for violating a rule, and report you. They will provide identification upon request.

<http://193.136.66.99/airobs/wp-content/uploads/2021/02/Schiphol-SafetySecurityPocketGuide.pdf>

You have a part to play in keeping Schiphol safe on a day-to-day basis. By following the security and safety rules you help ensure not only your own safety, but also the safety of your colleagues and of your customers. Schiphol safety is a team effort. This 'Safety & Security Pocket Guide' sets out the most important safety and security regulations in force at Amsterdam Airport Schiphol.

B.I. Otto

Executive Vice President & Chief Operations Officer Schiphol Group

Pocket Guide Safety & Security

As of 1 March 2024, the Safety & Security Pocket guide is no longer available. In preparation for the Safety & Security test to obtain a Schiphol pass, e-learning(s) are available in the Schiphol Learning Hub.

More information on the e-learning(s) can be found here →

learninghub-extern.schiphol.nl/uit/catalog/search/courses?query=security&limit=100&page=1&sort=Score_false&offset=0

security

Selecteer een categorie

Leeractiviteiten Leerpaden

Doelgroep

<input type="checkbox"/> Automatisering	0
<input type="checkbox"/> HRM	0
<input type="checkbox"/> Management	0
<input type="checkbox"/> Medewerkers werkzaam aan Airside	0
<input type="checkbox"/> Operationele medewerkers	1
<input type="checkbox"/> Schipholpasshouders	0

Werkvorm

<input type="checkbox"/> Blended learning	0
<input type="checkbox"/> Coaching / E-coaching	0
<input type="checkbox"/> E-learning	1
<input type="checkbox"/> Evenement	0

gevonden 2 items Sorteer op

Geen uitvoeringen

Training Security Awareness Experience Schiphol

In deze training worden de deelnemers mee genomen in de wereld van malware, phishing, kwetsbaarheden, exploits en data breaches.

Vergelijk Lees meer

Incompany € 0,00 Training



Training Security Awareness Experience

Incompany

Aanmelden interessant

Bewaar

Deel leeractiviteit

Deze leeractiviteit kan je gratis volgen

Leverancier
Schiphol

Leeractiviteit soort
Incompany

Bewijs na afronding
Bewijs van deelname

Aantal bijeenkomsten

Introductie

In deze training worden de deelnemers mee genomen in de wereld van malware, phishing, kwetsbaarheden, exploits en data breaches.

Doel

Wat zijn nu echt de risico's van onveilig online gedrag? Waarom is het gevaarlijk om zomaar op hyperlinks te klikken? Hoe herken je een phishingmail? Wat is een veilig wachtwoord? Waarom is het gevaarlijk om persoonlijke informatie op social media te delen? De Security Awareness Experience training geeft antwoord op deze vragen.

Tijdens de Security Awareness Experience training doorloopt een **ervaren** Certified Secure instructeur samen met de deelnemers een speciaal voor deze training ontwikkeld scenario. In dit zeer interactieve scenario **lopen de deelnemers zelf in de huid van een "hacker"** . De Certified Secure instructeur neemt de deelnemers mee in de wereld van malware, phishing, kwetsbaarheden, exploits en data breaches.

Tijdens de training wordt met behulp van **realistische** voorbeelden geïllustreerd hoe het onveilige gedrag van een **enkele** medewerker ernstige consequenties voor de gehele organisatie kan hebben. De deelnemers **ervaren** direct wat de impact kan zijn van een malwarebesmetting of het kiezen van een zwak wachtwoord. Door het gezamenlijk op een interactieve en praktische manier met security awareness bezig te zijn, **ontwikkelen de deelnemers de juiste Security Mindset.**

Programma

De volgende onderwerpen worden behandeld tijdens de training:

- Security Mindset
- Phishing herkennen en voorkomen
- Ransomware en malware
- Password breaches
- Het belang van software-updates
- Wachtwoorden, wachtzinnen en wachtwoordkluizen
- Online footprint (social media, Google)

Selecteer een plaats en datum

Kies een begin- en einddatum voor de zoekperiode

Er zijn geen uitvoeringen beschikbaar.



Uh oh..

Er is iets misgegaan. Neem contact op met onze IT-ServiceDesk (020 - 601 444 5) als het probleem aanhoudt. Gebruik onderstaande knop om snel weer terug te gaan naar de Schiphol Learning Hub.

Home

Terug

Class LMS is een product van Archipel Academy. Omdek [hier](#) meer!

Geen uitvoeringen



Training Hacker Mindset

Schiphol

In deze training krijgen de deelnemers een goed beeld van hoe hackers tegen beveiliging aankijken en welke mindset benodigd is om de risico's in de...

Vergelijk

[Lees meer](#)

Incompany € 0,00 Training

6 uitvoeringen



Training Schiphol Crisis Organisatie 1 (SCO1)

Schiphol

Maak je deel uit van de crisisorganisatie van Schiphol of ben je geïnteresseerd in de crisisorganisatie? Dan kan je deze opleiding volgen.

Vergelijk

[Lees meer](#)

Incompany € 0,00 Training

Een nieuwsgierige retorische vraag:
Waarom krijgt Schiphol Airport de beveiliging al zo lang niet daadwerkelijk op orde ?

Als je als snr security officer weer eens door de luchthaven Schiphol loopt, valt het al te vele jaren telkens weer op dat er zelfs wat basis beveiliging principes niet daadwerkelijk tot uitvoering blijken te komen.

Bijvoorbeeld:

q) 'security' medewerkers die schaamteloos gezellig over vertrouwelijke operationele zaken kletsend met elkaar, vanuit een publieke hal naar een beveiligde zone lopen dmv NFC pasje naast een toegang deur, en niet op of om kijken wie er achter hun aan mee naar binnen glipt.
r) een leverancier monteur van netwerk gekoppelde hardware devices, zonder begeleiding/toezicht van schiphol security medewerker, aan apparaten aan sleutelen is waar vertrouwelijke data doorheen gaat, op het scherm zichtbaar is dat met 'admin' rechten bezig is; even naar een andere plek lopen en daarvoor netjes screen lock activeren; maar vervolgens terug komen en voor iedere omstander zichtbaar de opvallend eenvoudige toegangscode invoeren (geen 2fa o.i.d.). Ook op een rol-kar de documentatie en opdracht bon laten liggen als er naar een andere plek (buiten zicht) heen en weer gelopen blijft worden.
Heb eens bekeken of dat apparaat en die leverancier überhaupt wel daadwerkelijk voldoen aan bijv een van de ISO27xxx normen, en dat blijkt niet het geval te zijn.

Dus, welke 'Security Officer' heeft er goedkeuring gegeven om dat maar aan de Schiphol netwerk infra te laten koppelen ?
s) wat Schiphol IT medewerkers via hun 'smart-phone' en/of tablet 'admin' toegang hebben tot delen van de vitale infra van de luchthaven, dmv een trust-relationship tussen apparaat en de infra (blind trust in somewhat dysfunctional IAM ?). En blijkbaar zich daar niet zo bewust van zijn welke gevolgen 't kan hebben als "iemand anders" het apparaat in handen krijgt, fysiek of covert-remote-digitaal. Tenminste, die indruk zou iemand kunnen krijgen als die ziet hoe roekeloos sommige medewerkers die apparaten 'even' onbeheerd laten rondslingeren of in de trein infra configuraties doen met omstanders die mee kunnen kijken.
t) het opvalt dat Schiphol Telematics (ST.nl), een wildgroei aan IT infra heeft laten ontstaan, waarbij het voorkomen van "attack surface" een ondergeschoven kindje blijkt te zijn bij het ijverige meer meer IT prestige projecten feest. De vragen "Is het überhaupt echt nodig!?" & "Kan 't ook veel veiliger en eenvoudiger binnen reeds bestaande elementen!? ipv weer iets er bij te gaan doen" lijken door geen CISO serieus op tafel gelegd te worden.

Ook blijkbaar wat "outsourcing" partners er wat met de pet naar te gooien, en ST blind te vertrouwen op beloftes op papier ipv gezond verstand controle [o.a. Cloudflare, Inc. & Pulsant Limited]

..)

z) dat het melden van een "security incident" bij een medewerker, best het ene oor in en het andere weer uit kan gaan zonder dat die medewerker de verplichte kleine moeite wil doen om het ook als incident te rapporteren of door te geven naar iemand die wel actie wil ondernemen. Met andere woorden, men blijkbaar meldingen niet zo serieus wil nemen als 't ze op dat moment persoonlijk niet uitkomt (zit immers geen beloning waardering aan gekoppeld om 't te doen).

*** in (z) zit 'm ook de crux als het gaat om waarom Schiphol management het alsmaar niet voor elkaar krijgt om de oh zo mooie woorden in beleidsdocumenten om te zetten naar een zichtbaar Functionele operationele structuur.**

Is natuurlijk ook voorspelbaar dat het mis blijft lopen als men bijvoorbeeld weet dat 'security officers' niet afgerekend/beloofd worden op tastbare resultaten maar alleen op de uurtjes dat ze 'werken'. Dat is vragen om struisvogel politiek en afschuiven van verantwoordelijkheden naar 'anderen'.

Neem bijvoorbeeld de huidige "Director Safety and Environment and CISO at Royal Schiphol Group" waarbij men het blijkbaar geen integriteit belangenverstrengeling lijkt te vinden dat iemand 2 petten op heeft waarbij er eigenlijk functiescheiding zou moeten zijn om te zorgen dat een slager niet zijn eigen vlees laat goedkeuren vanuit een machtspositie.
Wat ook opvalt is dat de "CISO" klaarblijkelijk zelf zich niet zo veel lijkt aan te trekken van "Security Awareness" Trainingen en essentiële beveiliging principes ? Althans, die indruk zou men kunnen krijgen als men ziet dat die persoon zonder schaamte roekeloos opvallend veel en gedetailleerde Informatie over zichzelf en de organisatie zo maar deelt met de wereld en hostile actors.
Daardoor zichzelf en de organisatie en de nationale vitale infrastructuur / staatsveiligheid roekeloos extra in gevaar brengt, wetende dat die informatie gebruikt wordt voor o.a.: Omkoping/Chantage; Profilering; Identiteit diefstal; Social Engineering; APT's via persoonlijke apparaten; Spionage & Sabotage; enz. ; enz..

:(linkedin.com/in/hedzer-komduur-39ba7a5/
"I am driven, like assessing the big picture, but also have a keen eye for details, both in business and in people."
* schiphol.nl/nl/schiphol-group/director-safety-en-environment/

Met andere woorden, het Schiphol bestuur het blijkbaar prima lijkt te vinden als de "Need to know" basis beveiliging regel compleet genegeerd mag worden, als het gaat om persoonlijke winst belangenverstrengelingen, zoals publiek opscheppen over hoe fantastisch men zou zijn voor een overbetaalde bureaucraat positie ?
Als men dan ook ziet hoe veel als vertrouwelijk geclassificeerd behorende INTERNE data de organisatie 24/7 naar het publieke internet lekt via vele wegen..., omdat/doordat de CISO en alle andere Security Officers er blijkbaar geen zin in hebben om er (naar wettelijke verplichtingen behorende) zeer eenvoudig voor te zorgen dat alle interne&gevoelige "meta-data" die niemand anders iets aan gaat, er uit gewist/gefilterd is alvorens computer bestanden en emails naar Buiten gaan. Zo ook nogal wat IT services producten die nog exact laten weten welke software en versie en security instellingen ze hebben, via netwerk communicatie protocollen roekeloos met de wereld gedeeld blijft worden, ondanks dat iedere security professional donders goet weet dat die informatie gebruikt wordt om specifieke kwetsbaarheden te vinden/identificeren voor gerichte long term covert intrusions. [*12] Als die extra details informatie hoeft helemaal niet beschikbaar gemaakt te worden, is immers verder nergens voor "nodig". => "Elementary, my dear Watson!"

Wat ook opvallend is, is dat er geen functioneel beleid met pro-active procedures actief blijkt te zijn om spionage en criminele infiltratie buiten de organisatie en infrastructuur te houden.
Ook op dat vlak zijn er vooral oh zo mooie PR type woorden op papier gezet, bijv: schiphol.nl/nl/werken-op-schiphol/pagina/help-onderneming-in-te-bestrijden/
Extra beschamende feit daarbij is dat die website waar naar verwezen is [www.sterkluchthaven.nl] zelf opvalt ivm gebrek aan voldoende aan wettelijke en beveiliging voorschriften.
Met andere woorden, een bureaukraat heeft 't bedacht en gemakzuchtig maar ergens over de schutting gegooid voor verdere uitvoering, Zonder de noodzakelijke controles uit te willen voeren?
? laat de slager z'n eigen vlees maar al te graag goedkeuren door slinks goedkeuring te "kopen" bij bedrijven die zogenaamde 'pen-test' en audits services verkopen (.met een uitkomst die de opdrachtgever wenst te krijgen..)

En zo zijn er nog wel wat observaties en bevindingen, als het gaat om een Machiavellisme spel dat roekeloos gespeeld blijkt te worden, ondanks dat het gaat om de veiligheid van ons allen zelf.

Waarbij men tot de conclusie zou kunnen komen dat de onderstaande vacatures er vooral zijn voor de "De nieuwe kleren van de keizer" Show, zoals uitvoering en handhaving verantwoordelijkheden steeds verder op alsmar meer sub-functionarissen af te schuiven, zonder tastbare resultaat verplichtingen.
Ipsa facto: Er een zwijgcultuur gecultiveerd blijkt te worden, in ruil voor een riant 'loon'.

--
https://careers.schipholgroup.com/vacatures/it-en-data/senior-cyber-security-manager
https://careers.schipholgroup.com/vacatures/it-en-data/cyber-security-manager
https://careers.schipholgroup.com/vacatures/security/security-process-developer
https://careers.schipholgroup.com/vacatures/security/security-auditor
https://careers.schipholgroup.com/vacatures/security/security-quality-training-manager
https://careers.schipholgroup.com/vacatures/techniek-en-bouw/strategic-advisor-center-of-excellence
https://careers.schipholgroup.com/vacatures/it-en-data/people-lead-asset-and-information-management-aim

https://careers.schipholgroup.com/vacatures/techniek-en-bouw/business-information-security-officer
+Begeleiden van eigenaren aangaande maatregelen ter versterking van cyberweerbaarheid.
+Vertalen van het security jaarplan naar concrete acties voor eigenaren.
+Verbeteren van (security) processen in het kader van de "PCDA"-cyclus.
+In kaart brengen van risico's en dreigingen bij diverse assets op IT en OT-gebied.
++Adviseren (gevraagd en ongevraagd) van de organisatie.
+Meedraaien in IT/OT projecten als vertegenwoordiging van security

?=> anw.ivdnt.org/article/zwijgcultuur

Maar hoe dan ook, C'est la vie.

? Mocht het zo zijn dat er iemand binnen het bestuur van Schiphol Group, of MinBZK, er wel degelijk waarde aan zou willen hechten om het Risicomanagement en Compliance op beveiliging van Luchthaven Schiphol, alsnog aantoonbaar naar behoren goed op orde te maken binnen korte tijd?

Dan kan dat zeer eenvoudig gerealiseerd worden door de huidige Ivoren Toren structuur CISO te vervangen, en er een type op die functie te zetten die wel vakkundig open en integer naar eer en geweten afgerekend/beloofd gaat worden puur en alleen op basis van daadwerkelijk onafhankelijke geteste/gecontroleerde resultaten.

Dus 0, krijgt en er uit vliegt, als blijkt dat de mooie woorden op papier niet daadwerkelijk waar gemaakt zijn.
Als een CISO persoonlijk Verantwoordelijk gesteld gaat worden voor feitelijke handhaving van uitvoering, gaat inherent Schiphol Luchthaven wel veel beter om met het beveiliging en compliance op orde krijgen en houden, toch ? ;)

Schiphol Group

Geen uitvoeringen

Catalogus

Jouw startpunt voor leren en ontwikkelen

Shape our Future - Reflective Leadership Training Schiphol

Deze eerste trainingsdag is bedoeld om je inzicht in je gedrag en het effect daarvan op medewerkers te vergroten. Je doorloopt verschillende situaties...

Vergelijk

Lees meer

Incompany € 0,00 Training





> On Wed, 12 Feb 2025 12:07:15 +0000
 > Juridisch <juridisch@onderzoeksraad.nl> wrote:
 >
 > Your message
 >
 > To: Juridisch
 > Subject: Re: Opvolging gesprek
 > Sent: Wednesday, February 12, 2025 11:07:24 AM (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
 >
 >> was read on Wednesday, February 12, 2025 1:07:15 PM (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna.

To: Juridisch <juridisch@onderzoeksraad.nl>
 Subject: Re: Read: Re: Opvolging gesprek

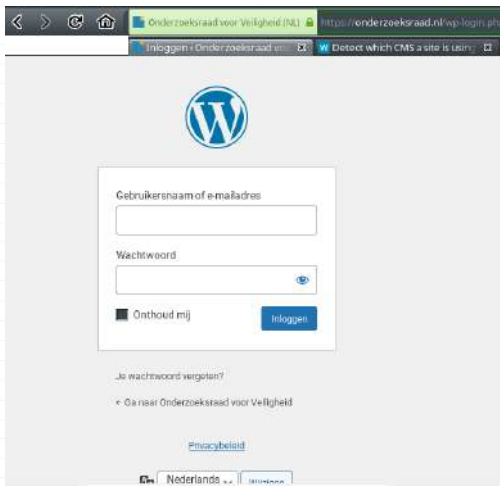
Is het "onderzoeksraad voor de veiligheid" bestuur nog van plan om iets zinvol te gaan ondernemen om die zeer ernstige misstand z.s.m. de nodige aandacht te gaan geven, alvorens 't nog erger mis loopt ?
 Of steekt men net als het Schiphol bestuur en NCTV en ILenT, de koppen liever bureaucratisch in 't warme zand, en roept men tzt "geen active herinnering aan"/"Wir haben es nicht gewut" als de media bekend maakt wat er gaande is en wie er Niet volgens taakbeschrijving in actie gekomen zijn...

Ter info:
 o.a. jullie website/webserver [onderzoeksraad.nl has address 85.209.110.220 @ Fundaments B.V.] is ook niet compliant met BIO, AVG, enz. Dus in overtreding van regelgeving veiligheid.
 Is zelfs al langere tijd volledige toegang door onbevoegden. Blijkbaar zonder dat men daar erg in heeft, of 't geheel niet interesseert ?

Men geeft dus zelf het verkeerde Voorbeeld, waardoor jullie adviezen ook niet zo serieus genomen kunnen worden?

Lijkt zelfs niemand een probleem te vinden dat o.a. deze (BBN2) vertrouwelijke data ook in handen van derden komt:
 ** <https://onderzoeksraad.nl/home/meldingen-luchtvaart/>

?-> onderzoeksraad.nl/home/werkwijze/informatie-verzamelen/



```
[+] WordPress version 6.6.2 identified (Outdated, released on 2024-09-10).
[+] Headers
| Interesting Entries:
| - Server: Apache
| - Content-Security-Policy: default-src * 'unsafe-eval' 'unsafe-inline' data: filesystem: about: blob: ws: wss;; base-uri 'self';
| - Referrer-Policy: origin-when-cross-origin
| - Feature-Policy: accelerometer 'none'; camera 'none'; geolocation 'none'; gyroscope 'none'; magnetometer 'none'; microphone 'none'; payment
'none'; usb 'none'
| +) sitepress-multilingual-cms
| Location: https://onderzoeksraad.nl/wp-content/plugins/sitepress-multilingual-cms/
|
| Version: 4.6.15 (100% confidence)
| Found By: Meta Generator (Passive Detection)
| - https://onderzoeksraad.nl/. Match: 'WPML ver:4.6.15 stt'
| Confirmed By: Readme - Stable Tag (Aggressive Detection)
| - https://onderzoeksraad.nl/wp-content/plugins/sitepress-multilingual-cms/readme.txt

[!] User(s) Identified:
[+] nover
[+] ingrid
[+] lisanne
[+] wp-zimpa
```



```
connect.onderzoeksraad.nl 77.242.112.135
mail.onderzoeksraad.nl 77.242.112.137
remote.onderzoeksraad.nl : 77.242.112.134
vpn.onderzoeksraad.nl 77.242.112.132
www.onderzoeksraad.nl 85.209.110.220 / 2a03:3400:8:200::2
www2.onderzoeksraad.nl ""
:(
```

Dictionary Thesaurus security Word of the Day

Dictionary

security noun

se-cu-ri-ty (sɪ-ˈkyʊr-ə-ti) -ˈkyʌr-

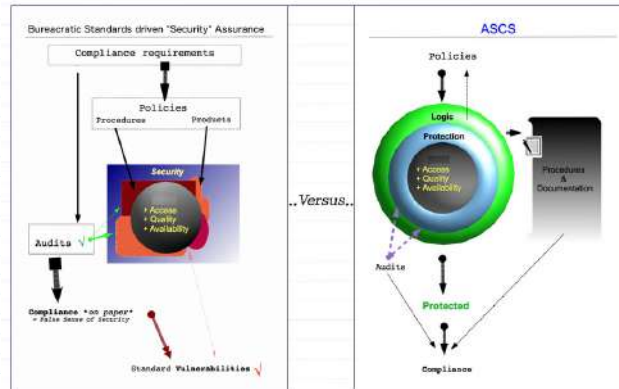
plural securities

Synonyms of security >

- 1 : the quality or state of being secure: such as
 - a : freedom from danger : SAFETY
 - b : freedom from fear or anxiety
 - c : freedom from the prospect of being laid off
 - job security
- 2 a : something given, deposited, or pledged to make certain the fulfillment of an obligation
- 3 : an instrument of investment in the form of a document (such as a stock certificate or bond) providing evidence of its ownership
- 4 a : something that secures : PROTECTION
 - b (1) : measures taken to guard against espionage or sabotage, crime, attack, or escape



Fixing the Risk-management => Security & Compliance issues, can only be done if.. C-Level management wants to allow it to be fixed.?
 # When it is allowed and sanctioned by leadership, then the structure can be corrected within ~1 year (without extra financial investments nor products)
 By using the simple "Safeguard"™ method. With full result warranty and open scope public verification.



- When choosing the *bureaucratic standards* driven "security" assurance approach, your organisation puts its own control & autonomy in 2nd place.
- **ASCS**, lets an organisation actually be in control of its self!

ASCS is a coherent method to melt the technology parts with group psychology & dynamics aspects of an organisation together in a self-balancing structure.

Side effects:

- Simplification of organisation and infrastructure
- Serious operational cost reductions
- Shorter change project turnaround
- Increasing in-house competence
- Inherent flexibility & resilience
- Justifiable best practice

Etymology

The name *Sciphol* appears in an official document from 1447.^[10]

11 September 1447.

*Gegeven in den Hage den XI^{ten} in Septembri ind jaer
ons Heeren duzent vierhondert seven ende veertich.*

HENRICH VAN BORSELEN, heer van *der Veere*, geeft, als
collator der kerk van *Aemstelerveen*, vergunning aan **REYNER
STREUYS**, pastoor dier kerk, om vier maden lands, liggende
5

66

in *Aelamerbanne* in *Schiphol*, te verkoopen en de opbrengst te
besteden tot de stichting van een nieuw kerkgebouw in plaats
van het oude, hetwelk vergaan is.

*Brief op verlannt met het zegel van den heer van
der Veere in rood was.
Archief, lokaal A 10, N. 3, 1.*



One of many explanations of the possible origin & meaning of the name:

Gathering wood

The word Schiphol first appears in old documents from around 1450 and refers to a stretch of land. This area was part of Aalsmeer, located south of Amstelveen, but was most certainly not a lake or sea. It was in fact a marshy area where people could go to gather wood. Schip-Holl dates from the 15th century and combines the Gothic words 'Schip' (meaning wood, timber) and 'Holl' (low-lying land). Later on a fort was also built on this spot, which carried the same name.

On September 19 in 1916, farmers in the vicinity of Fort Schiphol hear a strange hum in the air. A little later they see a plane landing, a Farman biplane of the Aviation Department of the Dutch Army. This is the beginning of Schiphol airport.