THALES
Building a future we can all trust

The 5 Cyber Tips for a Secure Supply Chain

The cybercrime will cost the global economy around **$5.2 trillion between 2020 and 2025**. Cybersecurity incidents today are in the **top 3 risks since the last 3 years***.

In that context, our clients and partners' security is our top priority. The following rules will both **enhance your company's resilience to cyber-attacks and strengthen the cyber-trust** with Thales.

Cooperation between Thales and its suppliers is key and can be built through:

- Answering a cyber maturity assessment questionnaire during the purchasing process,
- Taking into account new cyber contractual clauses,
- Initiating actions (if necessary) to improve your cyber resilience.

We thank you for your cooperation and full transparency.
Sincerely.

"Building a Future We Can All Trust, Together"

Roque Carmona
SVP Group Chief Procurement Officer

Stéphane Lenco
VP Group Chief Information Security Officer

*: respectively United Nations estimation and Davos World Economic Forum – The Global Risk Report 2018-2019-2020.

1 Define how you deal with cybersecurity

INFORMATION SECURITY POLICIES

Define **a set of cybersecurity rules** to **protect** your **information**, **product and services** against cybersecurity risks.

ORGANIZATION OF INFORMATION SECURITY

Appoint a **security manager** and identify **security point of contact** for Thales.

HUMAN RESOURCE SECURITY

Train your staff against cybersecurity rules.

2 Secure access to sites and protect data

PERSONAL DATA AND ASSET MANAGEMENT

Maintain an inventory of your assets and personnal data, to ensure their secure management.

PHYSICAL AND ENVIRONMENTAL SECURITY

Control access to your sites to prevent unauthorized access, physical damage or theft of information and tangible asset.

ACCESS CONTROL

Ensure that **all users** of your networks and devices **have unique** individual user **identifier** and use a **strong password**. **Administrator** privileges are limited to a **few people**.

3 Build and deliver cybersecure products and services

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

- Ensure that the **product or service you deliver** implements at least a set of basic **security design and coding rules** to prevent simple attacks from hackers.
- Make annual **vulnerability threat assessments** during product and services lifecycle.
- Provide **regular security updates** during products and services' lifecycle.
- Use **malware detection** tools for the exchanges between third parties and **before delivery**.

4 Protect the operations

OPERATIONS SECURITY

- Protect **all your systems and devices against malware** with the help of anti-virus solutions, and **keep them up-to-date**.
- **Record** security events, **monitor and audit** your systems to react in case of incident.
- Perform **regular security updates** on your systems and devices, following software providers' recommendations.

BUSINESS CONTINUITY MANAGEMENT

Deploy and **ensure business continuity and recovery** in case of a disaster.

5 Communicate

Pay particular attention

INFORMATION SECURITY INCIDENT MANAGEMENT

A **cyber incident** is likely to occur, no matter how careful you have been. **Be ready to communicate** this information **to your stakeholders, including Thales:** contact the **Thales CSIRT** (**Computer Security Incident Response Team**) at **cert@thalesgroup.com**.

Any of the following incident must be reported immediately:

- Cyber incidents, such as ransomwares, viruses, IT intrusions, CEO scam, suppliers' scam, which could impact the delivery of products/ services.
- Cyber incidents of any kind, which may spread to the Thales information systems / network and assets.
- Flaws and vulnerabilities, which could be discovered on the products and services already delivered to Thales.

Use the unique **global point of contact** to report cybersecurity incidents impacting any Thales entity: please contact the **Thales CSIRT** (**Computer Security Incident Response Team**) at cert@thalesgroup.com.

The headings refer to to ISO/IEC 27002:2014 chapters

THALES
Building a future we can all trust