Approved by the board on
22 November 2019

Cyber security policy

1. OBJECTIVE

This document outlines the cyber security policy within the Prosus Group, as a means to reinforce good governance by Group entities in a manner that is both agile and proportionate. The Prosus group means Prosus N.V. (Prosus) and their subsidiaries.

The policy is aligned with the group legal compliance, risk management, data privacy policies as well as with the group information and technology governance charter.

Our goal is that the practices outlined in this policy will support the cyber resilience of our businesses.

2. GROUP STATEMENT

Prosus is exposed to a wide range of cyber risks, some of which may have material and reputational consequence.

The group is committed to identifying and managing cyber risks as part of its Risk Management Framework (RMF) and in line with international best practices and regulations in the countries where it operates.

We acknowledge that no risk management system gives us absolute certainty that we fully understand all cyber risks or will avoid cyber-attacks. We will likely face cyber-attacks in the future, so we need to respond swiftly and stay resilient.

A one-size-fits-all approach to cyber resilience is not appropriate in the Prosus group as the businesses in the group are at various stages of maturity. As a consequence, our approach takes into account proportionality for the individual business, such as size and workforce, resources and complexity of activities.

Prosus expects businesses to focus on these four areas:

Governed Cyber Secure Cyber Vigilant Cyber Resilient

Each business should have IT and cyber governance in place which provides clear accountability. Each business should be able to identify/protect (Cyber Secure), detect (Cyber Vigilant), and respond (Cyber Resilient) to cyber attacks.

The amount of cyber controls and their breadth and depth will be decided by the businesses and will depend on their risk tolerance within Prosus group approved levels.

3. GOVERNED

Consistent with the group Information and Technology Governance Charter, individual businesses directly manage cyber security risk and IT operations.

The group provides oversight and guidance while also setting policy to ensure that activities happen within an approved framework.

The group periodically checks the security fitness of the businesses and requires biannual privacy and security status reports to group executives as an integral component of ongoing business reviews.

Each business should appoint a person who will be responsible for the implementation of this Policy and for cyber regulatory compliance within the relevant business or country. Such person should update the CEO and the CFO regularly on implementation. The largest businesses must appoint a Chief Information Security Officer ("CISO"). Below is an example of a possible distribution of responsibilities:

3.1. CTO, CISO or CIO

- Drives risk assessment with input of broader team
- Establishes a cyber risk management framework and relevant policies to implement the framework

- Provides cyber and IT systems and services
- Responsible for internal communication

3.2. **CFO:**

- Request audits of cyber resilience
- Procures cyber security insurance

3.3. **Legal**

- Provides legal advice on cyber security and data privacy
- Communicates legal requirements to internal stakeholders
- Establishes a privacy framework and relevant policies to implement the framework

3.4. **HR**

- Deploys employee trainings on security in the workplace

3.5. **CEO**

- Puts cyber risk resilience on management team agenda
- Ensures adequate crisis plan implemented and tested
- Ensures reasonable disaster recovery plan is in place
- Responsible for external communication

4. BASE PRACTICES

The Prosus group expects all businesses to address these ten (10) base practices. The depth and breadth of implementation will depend on the risk profile of the business and its maturity. If a base practice is not implemented, the business needs to provide rationale for the deviation.

Cyber Secure

- Risk Management
- Asset Management
- Identity and Access Management
- Security Awareness

Cyber Vigilant

- Log Management
- Continuous Monitoring
- Threat Intelligence

Cyber Resilient

- Backup Management
- Incident Management
- Crisis Management

4.1. CYBER SECURE

Businesses should mitigate known cyber threats to a level that would not result in material or debilitating loss for the business or significant brand/reputational damage.

The businesses should have sufficient knowledge and controls in place to ensure compliance with the regulatory requirements in the countries in which they operate.

At a minimum, it is expected that the businesses remain aware of the risks and assets they manage, that their employees remain aware of cyber threats and that the right access should be given to the right employees. The businesses should test robustness of these steps regularly.

Risk Management

The business is aware of the cyber risks and the risks are managed.

Asset Management

The business is aware of its IT and data assets.

Identity and Access Management

The business provides the need-to-know access only to authorized employees and third parties. Access is updated/changed and reviewed regularly.

Security Awareness

The business helps the employees and vendors to understand the cyber threats.

4.2. CYBER VIGILANT

Businesses should be able to detect cyber security events. At a minimum, it is expected that the businesses should be able to detect cyber-attacks on their assets and should have communication channels both within and outside the group that can alert to incoming cyber-attack or data leakage.

Log Management

The business maintains logs of security related system events.

Continuous Monitoring

The business proactively monitors the IT environment for potential cyber-attacks.

Threat Intelligence

The business works together with the group or external sources to proactively identify external cyber-attacks.

4.3. CYBER RESILIENT

Businesses should be able to quickly respond and recover from a cyber-attack.

Consistent with the group Data Privacy Program, each entity in the group is expected to define and implement an incident response plan that denotes the roles and responsibilities (and contact information) of key leaders tasked with managing data incidents broadly, and security incidents specifically.

At a minimum, it is expected that businesses should be able to restore their operations and have plans for incident and crisis management.

Backup Management

The critical business information is backed up and readily available in case of a disruption.

Incident Management

The business has plans how to handle a cyber incident and the team knows how to apply the plans.

Crisis Management

The business has plans how to handle a cyber crisis and management knows how to apply the plans.

5. CYBER INSURANCE

5.1. Cyber insurance

The group understands not all cyber risks can be mitigated to match the business, or segment risk appetite. Cyber insurance is one risk transfer mechanism currently available in the insurance marketplace.

5.2. Benefits

Other than balance sheet protection, cyber risk transfer solutions also provide our businesses with

- best in class advisors to promote and support incident response planning,
- help defend against or mitigate reputational damage, protect its directors from allegations of breach of duty and
- reinforce a culture of conducting annual cyber resilience reviews.

5.3. **Ownership**

The group internal insurance manager engages with the businesses to review and assist with their cyber insurance.

6. SUPPORT AND MONITORING

The I&T Governance Charter describes how our companies should assess, manage, and report on their IT related risk. group companies should use best practice frameworks to implement appropriate control measures.

The Prosus group's Internal Audit and Risk Support department helps businesses with their risk management activities through a dedicated cyber risk management team. In addition, and next to the individual business security activities, this department has its own services which provide objective assessments of cyber resilience of the businesses.

The audit committee and risk committee of the Prosus board of directors reviews and re-authorises this Security Policy and its implementation on an annual basis, as part of its oversight and governance responsibilities.

7. REPORTING

The following should be reported to head of internal audit and Prosus audit committee and risk committee:

- Significant cyber-attacks or breaches
- Significant breakdown in access controls
- Material risks and how they are mitigated
- Material risks that are not adequately mitigated.