Cyber security policy

Last reviewed and approved on 28 November 2023

NASPERS

Cyber security policy

1. OBJECTIVE

This document outlines the cyber security policy within the Naspers Group, as a means to reinforce good governance by Group entities in a manner that is both agile and proportionate. The Naspers group means Naspers Limited (Naspers) 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 competencies outlined in this policy will support the cyber resilience of our businesses. This security policy applies to all business assets, including platforms and business IT of our subsidiary companies. Directors on the boards and management involved with our minority investees should understand this policy and work with investees to adopt appropriate cyber security policies. To the extent policies in non-controlled investees are considered inappropriate this should be reported to the segment CEO, CFO and CTO.

2. GROUP STATEMENT

Naspers 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 Naspers 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.

Naspers expects businesses to focus on these four areas:

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 profile. In the case an outsourcing arrangement exists (e.g. SaaS), the business remains accountable for ensuring that their providers manage security in line with the expectations of this policy.

3. GOVERNED

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

The group (through its Risk & Audit function) monitors the security fitness of the businesses, inter alia by aggregation of periodic status reports from the risk functions, the CTOs, and Heads of Security, which is shared with the group executives and the risk committee.

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 supported by appropriate budget and staffing allocation, should update the CEO and the CFO regularly on implementation. In the largest businesses, this individual serves as a dedicated must appoint a Chief Information Security Officer ("CISO"), Head of Security or similar.

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

- Oversees the company's cyber security posture
- Ensures adequate crisis plan implemented and tested
- Ensures reasonable disaster recovery plan is in place
- Establishes need for / approves employee trainings on security
- Responsible for external communication

4. SECURITY COMPETENCIES

The Naspers group expects all businesses to build these ten (10) competencies.

Cyber Secure

- Risk Management
- Asset Management
- Identity and Access Management (IAM)
- Security Awareness
- Secure development

Cyber Vigilant

- Log Management
- Continuous Monitoring
- Threat Intelligence

Cyber Resilient

- Backup Management
- Incident And Crisis Management

The level of maturity of the competencies will depend on the risk profile of the business and its maturity. If a competency does not exist at a business, the business needs to provide a rationale for the deviation.

Five of these competencies are core competencies that mitigate the majority of the risks. These are IAM, Secure Development, Backup Management, Log Management and Incident and Crisis Management. All businesses need to have

well-defined controls (and associated KPIs) in place for these core competencies and implement the controls across the entire environment. The control implementation should prioritise the platforms that generate the revenue and the financial applications that support the business operations.

The controls for the core competencies will be subject to required combined assurance (e.g. audit by Risk & Audit) and should be assessed by the security teams of the business and Naspers group regularly.

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.

The businesses should remain aware of the risks and assets they manage.

In addition, the business needs to make sure that its employees remain aware of cyber threats and that the right access should be given to the right employees.

Finally, when the business develops new applications or features on its platform, the development needs to follow a strict change management process andto try and ensure no faulty or vulnerable code is introduced.

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 CORE COMPETENCY

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.

Secure Development CORE COMPETENCY

The business integrates security practices into the software development lifecycle and verifies the security of internally developed applications before they are deployed.

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 CORE COMPETENCY

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-incident.

Consistent with the group Data Privacy Program and Governance Policy, 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 CORE COMPETENCY

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

Incident and Crisis Management CORE COMPETENCY

The business has plans how to handle a cyber incident and the team knows how to apply them. Crisis management plan is in place and management knows how to apply it.

In the case a business is attacked by ransomware, the ransomware addendum to this policy equally applies.

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 conducting annual cyber resilience reviews.

5.3 Ownership

The group's head of insurance engages with the businesses to review and assist with their cyber insurance.

6. SUPPORT AND MONITORING

The Information and Technology 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 Naspers 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 Naspers board of directors reviews and re-authorises this Cyber 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 the Cyber Team of Risk & Audit. The team aggregates the results and shares them with the group CFO, the Governance Committee, and Naspers 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.

8. RESOURCES

This policy – including its ransomware addendum – references the following [Naspers][Prosus] policies:

- Risk Management Policy
- Data Privacy Governance Policy
- Information and Technology Governance Charter

NASPERS

Addendum: Ransomware

The competencies outlined in this addendum are intended to support the resilience and response of our businesses when faced with a ransomware attack, and to articulate Prosus' expectations for sound crisis management in this context.

Ransomware may cause severe disruption to business operations or, in extreme cases, halt a business. In a ransomware attack, an attacker obtains access to the internal systems and encrypts all the information. In some cases, the attacker also exfiltrates sensitive information from the business. To decrypt the information or return the stolen information, the attacker asks for a ransom.

In a response to this threat, the group adopted the following statement:

Prosus and the businesses within the Group will not consider the payment of a ransom as long as they are able to recover the business operations.

However, should Prosus and the businesses within the Group consider payment of any ransom, this will be subject to board approval.

Below we highlight in greater detail controls that should be included as part of the resilience competence (**backup management** and **incident and crisis management**) by every business, to ensure a business can recover from a ransomware attack.

BACKUP MANAGEMENT

Each business should have robust backup management in place. The backups should include all the systems that enable the business to operate. These are the platforms (for e.g. client databases, source code, infrastructure as a code and other configuration files) and backend systems. For SaaS services, the requirements should be articulated through service level agreements with the provider.

1. The systems should be regularly backed up.
    - 1.1. The backups should be immutable.
    - 1.2. The backup recovery times should be agreed with the business.
    - 1.3. The backup restoration should be regularly tested.
    - 1.4. The backups should be in a separate location and managed through a different account than the production environment.
    - 1.5. Access to the backups environment should be strictly managed
2. No person with access to the production environment should have access to the backup environment.
    - 2.1. No person with access to the backup environment should have access to the production environment.
    - 2.2. The access management of the backup environment should be implemented using best security practices (such as 2-Factor Authentication, complex passwords, regular password rotation) and access should be given to a limited number of people.

INCIDENT AND CRISIS MANAGEMENT

Each business should develop a ransomware playbook. The playbook should be closely linked to and consistent with the incident and crisis management processes of the business and highlight specifically the planned response of the

business against a ransomware attack.

To support the businesses, Prosus created a sample playbook that can be adapted and adopted.

If a business is targeted by a ransomware attack, it must promptly report it to the Prosus Cyber Team, who will notify appropriate stakeholders at Prosus. No interaction should be made with the attackers before completing this step. The team can be reached at: cyber@prosus.com.