CYBERSECURITY POLICY

SECURITY AT NRB: A PRIORITY

NRB hosts and supports the IT systems of organisations that are essential to the functioning of our country, whether in the public, private or healthcare sectors. We, therefore, have a crucial responsibility to ensure the continuity and quality of our services. The security of information systems and data is therefore one of the priority elements in the provision of our services to our customers and in the protection of our infrastructures.

HOW CAN NRB HELP PROTECT ITS CUSTOMERS FROM CYBER THREATS?

- By giving them confidence through our ISO27001 certification. This certificate, awarded by an independent auditing company, is proof of the integration of security into the organisation and of the implementation of measures to maintain the confidentiality, integrity and availability of data.
- By using a framework that covers all aspects of security, allowing NRB to respond to current and future threats.

Source : NIST

THIS FRAMEWORK IS BASED ON FIVE FUNCTIONS. THESE ALLOW TO ORGANISE THE CYBERSECURITY ACTIVITIES:

Identify: Develop a common understanding to manage risks on data, assets and systems.

Protect: Develop and implement appropriate countermeasures to ensure the protection and availability of critical services.

Detect: Develop and implement activities to detect the occurrence of cybersecurity events.

React: Develop and implement appropriate activities to follow up on a detected cybersecurity event.

Recover: Develop and implement appropriate activities to maintain resilience and restore services and data disrupted by a cybersecurity event.

HOW IS THIS FRAMEWORK IMPLEMENTED AT NRB?

FONCTION	OBJECTIFS ET ACTIVITÉS
Identify	- NRB has a security policy and an organisation with three lines of defence (Operational Security, Governance/Piloting and Internal Audit) - NRB complies with GDPR*/NIS*/ISO27001. - NRB has a risk management process with its own methodology based on ISO27005, recurring analyses and action plans. - NRB conducts an ongoing assessment of emerging cyber threats. - Based on the information provided by the client, NRB integrates the client's critical services and assets into its processes. - Together with the customer, NRB defines the organisation and communication channels with regard to safety.
Protect	- NRB's Data Centres have been designed and are operated to ensure security and continuity (Tier 3+ Uptime Institute level). - Data storage is secured with encryption. - The data is saved, and the integrity of the backups is checked. - Disaster Recovery plans are in place and, at least annually, tested - Hardening and patching are ensured through our vulnerability management process. - All NRB employees undergo continuous safety training.
Detect	- The NRB network is permanently monitored, and any abnormal behaviour with respect to the defined baselines generates an alert. - End-user activities are monitored to detect abnormal access attempts. - Security events are collected from critical sources and correlated by our 'Security Information and Event Management' tool. - Security events and alerts are analysed 24/7 by our Security Operation Center. - Anti-malware is active on workstations, mail/web gateways and firewalls. - Vulnerability scans are performed on a recurring basis.

React	- NRB has incident and crisis management processes in place to deal effectively with cyber incidents and ensure continuity of services. - NRB is in contact with partners (Cert.be, CCB, MSSP) to share information about threats and incidents. - NRB carries out forensic investigations and analyses in collaboration with external specialist service providers. - Incidents are analysed and categorised in order to execute predefined action plans. - Incidents are confined and mitigated to limit their impact.
Retrieve	- Recovery plans are executed during or after the incident is resolved. - Relations with external parties are managed as part of the crisis process. - After resolution and recovery, incidents and actions taken are analysed to improve management processes and action plans.

*GDPR (General Data Protection Regulations): The purpose of the GDPR is to provide a framework for practices relating to the collection, processing and use of personal data.

*NIS (Network and Information System Security): The NIS Directive is a regulatory framework to strengthen the cybersecurity of Digital Service Providers (DSPs), i.e. mainly cloud and search engine companies.