BNY

CYBERSECURITY PROGRAM OVERVIEW

January 2025

Introduction

BNY has developed cybersecurity strategy, policies and standards for the secure control, processing, storage, transmission and communication of information. This document summarizes the general statements of the BNY cybersecurity policy which is intended to comply with the different regulatory requirements across geographies.

Our Cybersecurity Strategy

Technology enables a world of possibility for financial services institutions but also exposes companies to attacks by sophisticated adversaries. Today's cybersecurity threat landscape encompasses a vast array of evolving risks and exposures: nation-states seeking to steal and exploit intellectual property and insights; hacktivists aiming to cripple services to inflict reputational damage, and criminal enterprises and insiders working for financial gain.

BNY takes these risks seriously. Protecting the confidentiality, integrity and availability of information is paramount to our business and clients – and reinforces our corporate principles.

We have invested in evolving our cybersecurity program – developing our people, processes, and systems. Every user at BNY is required to take the company's Cybersecurity Awareness training, which covers password security and management, device security, safe operating habits, information classification and handling, reporting suspicious activities, and more. We have in place multiple levels of IT-related threat protection and preemptive computer security measures designed to protect the company and our clients. We perform phishing testing at least quarterly and participate in industry exercises to ensure integration with market partners. Protecting our information requires a strong defense on all fronts, from building on our dynamic cybersecurity strategy to developing, implementing and managing comprehensive controls and information security services.

Our cybersecurity program is designed to anticipate, and effectively respond to, cybersecurity threats and their diverse, multifaceted attacks. It is closely aligned with the Enterprise Resiliency Office, which coordinates the company's approach to incident and crisis management, business continuity and disaster recovery.

Our Cybersecurity Approach

Our cybersecurity program is aligned with leading standards such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and is ISO 27001 certified by the International Organization for Standardization. BNY is independently audited for its Centrally Managed Information Technology Services (CMITS), Service Organization Control Report (SOC1SM), and Sarbanes-Oxley (SOX) controls. The control tests in these reviews align with many of the Control Objectives for Information and Related Technology (COBIT) standards for Information Risk and Control Governance, providing an independent evaluation of fairness on the presentation, design, and effectiveness of our internal control environment.

In addition to a multi-layered control infrastructure with built-in redundancies and checks, our program:

- Includes comprehensive global, risk-based policies and standards for the control, processing, storage, transmission and communication of information.
- Leverages threat intelligence capabilities that aid investigations and inform key business decisions.
- Monitors our enterprise for vulnerabilities and risks and rapidly responds to threats.
- Evolves our cybersecurity and risk management program to stay ahead of the dynamic threat landscape.
- Collaborates across our businesses, technology, risk, compliance and internal audit organizations to implement a consistent and transparent approach.

ISO 27001 Certificate

BNY holds ISO 27001 Certification of its Information Security Management System framework, including but not limited to:

- Antivirus Management
- Asset Management
- Backup & Restoration Management
- Capacity Management
- Change Management
- Compliance
- Cryptography
- Data Centers
- Desktop Security
- HR Security
- Incident / Problem Management
- Information Security Continuity
- Information Security Policies
- Information Systems Audit Controls
- Logging & Monitoring
- Network Devices
- Organization of Information Security
- Patch Management
- Physical Security
- Remote Access Management
- Supplier Management
- Transport and Storage of Media
- User Access Management
- Vulnerability Management

Cybersecurity Policies Applicability & Scope

The Cybersecurity Policy applies to BNY and its affiliates. To maintain confidentiality, integrity and availability of company information, all permanent and temporary employees and contractors at BNY – including those from subsidiaries and third parties to BNY or its affiliates – must comply with the Cybersecurity Policy and any related policies, standards, guidelines and procedures developed by the business unit.

Cybersecurity Policy Summary

The Cybersecurity Policy outlines our cybersecurity program and related policies and standards. Cybersecurity includes the practices and processes used to protect corporate information, including the confidentiality, integrity and availability of information from damage caused by electronic means. In addition, cybersecurity encompasses controls aimed to maintain the accessibility and resilience of applications, systems, networks, and other infrastructure elements that support the maintenance of corporate information.

The BNY cybersecurity program is supported by a governance framework, which includes, but is not limited to, various policies, standards, and procedures each covering key related disciplines – in addition to a robust cybersecurity awareness program.

This document provides a summary of the key security capabilities covered in our Cybersecurity Policy.

> **Cybersecurity Governance** establishes the controls and processes to comply with cybersecurity, information protection, privacy, regulatory and legal requirements to respond to scenarios involving cyber threats. Education and awareness programs are part of the BNY governance process.

> **Vulnerability Management** is defined and operated to identify, quantify, classify, prioritize, and address vulnerabilities in any systems, networks, or applications with access to enterprise data – both in transit and at rest.

- **Application Security** strives to reduce risk by improving the security profile of high-risk applications. This is achieved through a formalized program integrated with each phase of the development life cycle and promotes cooperation between Application Development and Application Security.
- **Security Monitoring & Logs** are defined and operated to identify and respond to suspicious or malicious activities or incidents in the BNY technology environment. Detected atypical activities are directed for analysis by the incident response team.
- **Physical & Environmental Security** consists of security processes and controls defined to help ensure that technology assets are protected against unauthorized access, loss, damage or theft.
- **Information Protection & Encryption** consists of information protection processes and controls defined and operated to preserve confidentiality, integrity, and availability and protect against unauthorized access, use, disclosure, interruption, modification, collection, leakage, or destruction of information.
- **Information Classification** requires that all data and information possessed by BNY or under company control, including information received from sources outside of BNY such as supplier and client data, must be classified as Highly Confidential, Confidential, Internal Use Only, or Public.
- **Identity & Access Management** helps ensure access is provisioned, approved, maintained, periodically reviewed, and disabled or removed in compliance with the principles of least privilege and segregation of duties. Authentication and password protection parameters are defined and operated to protect against unauthorized use of – or access to – BNY technology assets or information.
- **Cyber Incident Response** is operated to identify, analyze, manage, and investigate suspicious activity and cyber incidents. Incidents are managed and handled in compliance with the BNY cyber incident response program.
- **Third-Party Service Provider and Vendor Management** helps ensure and verify that third-party contractors or vendor partners implement processes and controls that, at a minimum, are equal in effectiveness to BNY controls and processes in protecting the organization's information, resiliency, and compliance with any regulatory requirements.
- In the **Container Security** process, all architectural risks are identified, evaluated, and addressed.
- The **Security in the Card Payment Industry** (PCI-DSS) program helps ensure appropriate encryption standards and tools are implemented to protect the confidentiality, authenticity, and integrity of data in transit or at rest. In addition, preventive and detective processes are implemented to manage data leakage or loss.
- **Security on Mobile or Portable Devices** follows guidelines for settings and protection of data and equipment, as determined in policies and procedures specific to these features.
- BNY considers insider threats to be a serious matter. The **enterprise-wide Insider Threat program** provides direction, governance, and organizational awareness to manage risks, aligning to the company's organizational risk priorities, which include enhanced protection of information assets.

Governance & Responsibilities

BNY has teams and individuals responsible for maintaining, implementing, and adhering to the responsibilities of the Cybersecurity Policy. As a sample, there is the Chief Information Officer, Chief Information Security Officer, Technology Control Management, Operations and Technology Governance and business information security officers.

Adherence & Controls

Failure to comply with the Cybersecurity Policy may result in disciplinary action, and exceptions may be reviewed and granted in accordance with internal policies and procedures.

General Note

The Cybersecurity Policy may be changed whenever necessary by the individuals or responsible teams who identify any risk or threat not contemplated in this document.