Corporate Policy No. 21: Incident and Breach Response Policy Statement

Date Established: 20-Feb-2024
Data Last Update: 27-Mar-2025
Version: 1.1

OUR POLICY COMMITMENT

At Dun & Bradstreet (D&B), we recognize that timely detection and management of incidents is a key component of mitigating regulatory, compliance, cybersecurity, fraud, and other risks. We are committed to effectively managing these risks as part of our commitment to responsible data processing. We extend this commitment to our customers and users of our solutions and services through contracts and other written agreements. As part of this commitment, we maintain a comprehensive Global Compliance and Ethics Program and a Cybersecurity Program, for which our incident response standards and processes are a key component of preventing, managing, and mitigating regulatory, compliance, and cyber risks. We align our Incident and Breach Response standards with our Corporate Policy Statement on Speak Up and Non-Retaliation to support our commitment to a speak up and non-retaliation culture, and where applicable, to our Crisis Management processes.

This Policy Statement summarizes our baseline principles and operating standards for managing our response to data, compliance, and security incidents in connection with the components of our comprehensive Global Compliance and Ethics program and our Cybersecurity program. It provides a framework for compliance and effective risk management under privacy, data protection, consumer protection, data and cybersecurity, and breach notification laws, rules, and regulations globally. This Policy sets the baseline requirements for detecting, responding to, managing, and reporting data, compliance and security incidents at D&B. Where an applicable law, rule, regulation, or contractual obligation requires a higher standard, we will follow the requirements of that law, rule, regulation, or contract.

WHAT DO I NEED TO KNOW AND DO

The following 6 Principles and Operating Standards guide the way we work to meet our Policy Commitment. Each of these core Principles and Operating Standards are relevant to all D&B team members. Among these Standards, the most important step is that all team members promptly report every event that they suspect to be (or could lead to) an Incident.

1. **Incident Types and Categories:** D&B categorizes incidents into three groups: Data-Related Incidents, System-Related Incidents, and Compliance Incidents. You are responsible for knowing the types of incidents that fall into these groups so that you can support our commitment to timely detecting and managing these incidents.
2. **Incident Severity levels –** In order to appropriately manage D&B's response to incidents, all Incidents are assigned a severity level based on the potential for adverse impact to D&B, or to other individuals or organizations. You should be aware of the Incident severity levels and the different response, management, and reporting that must be followed based on severity levels.
3. **Incident Response Process:** The Incident Response process is coordinated by the Incident Response Team under the direction of the Chief Cyber Security and Technology Risk Officer and Chief Ethics & Compliance Officer. It encompasses six (6) phases comprised of preparation; detection; reporting and escalation; analysis and evaluation; response; and post incident activities.
    a. **Reporting and Escalation:** Team members must promptly report all actual and suspected Incidents, including events and occurrences suspected to be Incidents, to the Incident Response Team. Third Parties must report all Incidents and Data Breaches in accordance with the terms of the applicable agreement(s) between D&B and the Third Party. **For Incidents to be deemed appropriately reported in compliance with this Policy, they must be reported or escalated to incident@dnb.com**. Additional intermediary reporting channels are described in the full Policy.
4. **Incident Management and Communications:** Decisions regarding the management and communication of Incidents following the Initial Evaluation shall be based on the Severity of the Incident.
5. **External Reporting** – Various privacy, data protection, data security and other laws, regulations, and government orders applicable to D&B require different forms of notification or reporting of certain Incidents to regulatory authorities and other stakeholders. D&B will report Data Breaches and other Incidents to regulatory authorities and other stakeholders in accordance with the requirements of applicable laws, regulations, and government orders, which may change from time to time.
6. **Record Keeping** – D&B maintains a central repository for records related to Incident and Regulatory Reporting.