IT Security Incident Reporting and Response Policy

Issued April 1, 2022

.010 Purpose

This policy governs the actions required for reporting or responding to security incidents involving F1 TEAM information and/or information technology resources to ensure effective and consistent reporting and handling of such events.
.020 Scope

This policy applies to all members of the F1 TEAM community, including students, personnel, units, and affiliates using F1 TEAM information technology resources or data.
.030 Effective Date

This policy became effective on January 8, 2001 .040 Authority

For major incidents, which include a breach of personal identity information (PII), policy requires escalation to the top administration and prompt notification of the Board of Directors office.

.050 Policy
All members of the F1 TEAM community are responsible for reporting known or suspected information or information technology security incidents. All security incidents at F1 TEAM must be promptly reported to Generic Company's Chief Information Security Officer (CISO) and other appropriate authority(ies) as outlined below in Section .080: Implementing Procedures.
Incident response will be handled appropriately based on the type and severity of the incident in accordance with the Incident Response Summary Table below in Section .080: B.2 and Generic Company's IT Security Incident Management Procedures. Handling of security incidents involving confidential data will be overseen by an Executive Team.
All individuals involved in investigating a security incident should maintain confidentiality, unless the manager on duty authorizes information disclosure.
.060 Definitions

Security incident- Any real or suspected event that may adversely affect the security of F1 TEAM information or the systems that process, store, or transmit that information.

.070 Roles and Responsibilities

The incident manager is responsible for managing the response to a security incident as defined in the incident response summary table in Section .080.B.2 below.
The Executive Incident Management Team oversees the handling of security incidents involving confidential data (e.g., personal identity information). This team has authority to make decisions related to the incident and to notify appropriate parties. The team consists of:
Senior administrator for the affected unit Chief Information Officer
Chief Information Security Officer Representative from the Office of General Counsel
Assistant Vice President for Media Relations Others as needed (for example, F1 TEAM Police for criminal incidents)

.080 Implementing Procedures

Reporting Security incidents
Any member of the Generic Company community who suspects the occurrence of a security incident must report incidents through the following channels:
All suspected low severity events as defined in Section .080.B.1 below , including those involving possible breaches of personal identity information, must be reported directly to the Chief Information Security Officer (CISO) as quickly as possible by phone (preferred), e-mail, or in person. If the CISO cannot be reached, contact the Chief Information Officer (CIO).

Responding to Security Incidents
Incident Severity
Incident response will be managed based on the level of severity of the incident.
The level of severity is a measure of its impact on or threat to the operation or integrity of the institution and its information. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of incident severity will be used to guide incident response: high, medium, low, and NA (Not Applicable).