Incident Response – Lost/Stolen Device

Purpose:
The purpose of this document is to provide guidance to IT Custodians of individual Biological Sciences Division (BSD) Departments of the potential information required from IT Custodians to be given to Security Analysts upon a Potential Security Event realized as a **Lost/Stolen Device**.

Scope:
This cheat sheet describes the questions a Security Analyst will be requiring to answer based on a Potential Security Event turning into a Lost/Stolen Device Incident and the potential actions a Security Analyst will require an IT Custodian to perform to contain, eradicate and remediate a Lost/Stolen Device Incident.

Roles:

Role	Description
IT Custodian	Responsible for managing IT systems assigned to them within their department. Typically, the first connect for end-user experiencing a potential incident.
BSD ISO Security Analyst	The BSD Information Security Office (ISO) provides information security services and security guidance to the BSD leadership and all members of the BSD research and academic enterprise. The Security Analysts within the BSD monitors events throughout the BSD departments and determine if potential incidents should be escalated to incidents. The BSD ISO works with end users, IT Custodians, and leadership within the BSD to ensure incidents are resolved in a timely manner.
System Owner	A System Owner is an employee of the BSD who is director level, faculty, or above who has the ultimate responsibility over a particular IT system. System Owners are responsible for ensuring their systems are maintained in a secure manner and working with IT Custodians and the BSD ISO to ensure security incidents are resolved in a timely manner.
Unit Leader (UL)	Unit leaders are senior leaders within each department. ULs are responsible for ensuring their departments operate within the BSD guidelines and policy, including security. ULs are the third level of escalation for security incidents and are typically only notified when all other means of resolving the security incident are exhausted.
BSD Chief Information Security Officer (CISO)	The BSD Chief Information Security Officer (CISO) is the lead of the BSD ISO. The CISO is responsible for developing, and maintaining security policies, standards, and procedures across all the BSD departments. The CISO facilitates the escalation of security incidents when initial attempts to correct the incident are exhausted and the security incident has not been resolved.

Incident Response – Lost/Stolen Device

(LOST/STOLEN DEVICE CATEGORY)

Upon notification that a Potential Security Event has been promoted to a Lost/Stolen Device Incident, the Security Analyst is required to answer the following questions or provide the following requirements:

Questions/Requirements	Actions/Answers
Was tracking software installed and enabled?	Upon the realization of a device being Lost or Stolen, the BSD ISO will need to know if tracking software was installed: **Yes/No**
Can equipment be located and re-acquired?	**Yes/No**
If equipment cannot be re-acquired…	...BSD ISO Security Analyst will require the following information: **Lost/Stolen Police Report ID:** **Lost/Stolen Police Organization contacted:** **Date the Lost/Stolen Police Report was filed:**
Was equipment signed in when lost/stolen? (information from user)	**Yes/No**
Was the equipment encrypted?	**Yes/No** If "yes", please inform Security Analyst how and if there is evidence, please supply the security analyst a screenshot of the proof.
Was sensitive data on the eqiuipment?	**Yes/No**
Was any data lost?	**Yes/No**
Are backups available?	**Yes/No** If "Yes", then what is the date when the data restored from backup? If "Yes", then what is the date when the data was restored on replacement?