Incident Response – Data Breach

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 **Data Breach**.

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

(DATA BREACH CATAGORY)

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

Questions/Requirements	**Actions/Answers**
Classification of Data Breached:	**Personal Information/PHI/PII/Research**
Amount of Data Lost due to the Data Breach:	**# of Records or amount of data**
Has the information lost due to the Data Breach been released publicly?	**Yes/No**
Is Data Still being exfiltrated?	**Yes/No** If "yes", then what is node still sending data? If "yes", then what is the data that the node was isolated from the network? If "yes", then what remediation actions were conducted to stop the data breach and to prevent it from occurring in the future?
Are credentials compromised due to the Data Breach?	**Yes/No** If "Yes", then what is the date that the offending user's account password was changed?
Have stakeholders determined that external notification is necessary?	**Yes/No**
Did data breach occur as a result of a phishing campaign?	**Yes/No**
Did data breach occur as a result of malware?	**Yes/No**