SECURITY INCIDENT RESPONSE MATRIX

IT Security Incidents

IT Security Incident - The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

Incident Type	Name	Description of Incident	Reporting Timeframe
Incident 1	Theft	Any type of theft of an IT resource. Including removable/flash drives, software, hardware, PC's, laptops or phones.	Immediately
Incident 2	Unauthorized Access	Any type of un-authorized access to any IT resource or asset.	Within 24 hours
Incident 3	Denial of Service	Any attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This includes being the victim or participating in a DOS.	Immediately
Incident 4	Malicious Code Execution	Any successful installation of malicious software (e.g., virus, worm, trojan horse or other code based malicious entity) that infects an operating system or application.	Within 24 hours
Incident 5	Improper Usage	A person violates acceptable computer usage policies.	Within 5 days
Incident 6	Scans/Probes/Attempted Access	Any activity that seeks to access or identify a computer, open ports, protocols, service or any combination for later exploitation.	Within 5 days
Incident 7	Service Unavailable	When any service or application (e.g., email, internet, Affinity) is unavailable for use over a period of time.	Within 24 hours