UMKC Information Security Incident Reporting

What is Information Security Incident Reporting?

Information Security Incident reporting is the process of collecting and reporting suspicious, inappropriate, or unauthorized activity related to University electronic systems and data. This includes but is not limited to suspected account abuse, data theft, data loss (such as loss of a memory key with sensitive information), and system security breaches. More information on what must be reported is at the ***UM Mandatory Reporting Requirement page***.

What is the timeline for reporting an incident?

Physical security incidents (such as theft and break-in) should be reported immediately to the Campus Police, then reported to Information Services. All other incidents should be reported to Information Services immediately.

Why is it Important?

Information Security Incident Reporting is a mandatory reporting requirement within the University of Missouri. This allows us to track incidents, remediate affected systems, and follow other mandatory processes related to risk of data loss. This also allows us to track patterns of data loss due to certain types of attacks.

How do I report an incident?

All Information Security Incidents should be called in to the UMKC Call Center at 816-235-2000 or sent in by email at techsupportcenter@umkc.edu . After an initial ticket has been opened, the Information Security team will contact you to follow up for further information.

When reporting an incident, provide as much detail as possible. This includes information on:

- What has physically happened (such as in the event of a laptop theft, or finding key-logging hardware attached to a machine, etc.)
- Why you suspect data theft/abuse (such as finding personal documents tampered with, sensitive data modified, etc.)
- When you suspect the incident occurred (such as the date a modified document was last known to have correct data)
- Where the incident may have occurred

All physical incidents such as laptop theft should first be reported to the Campus Police, with a follow up report as a Information Security Incident.