Security Incidents

Reporting Security Incidents

If you've lost a device or suspect a security incident has occurred, report it to the service desk right away!

Report a Sec

How to Report a Security Incident

UCAR employees can report potential cyber events and incidents in several ways including by email, phone, or in-person.

Anonymous report submissions regarding issues affecting UCAR or UCAR systems can be made using the UCAR Ethicspoint Hotline. More information is available on our Ethics page.

Learn More

Use the button below to login to the Wiki and learn more about our Incident Response Plan.

Review Incident I

Types of Security Incidents

A security incident is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.

Incident Type	Description
Lost of Stolen Device	An organization-owned device, or a personal device with organization credentials or data, is stolen or lost.
Phishing Attack	A form of “social engineering” when deception is used, usually through email or phone, to steal information such as credentials, bank account numbers, social security numbers, or to convince the recipient to perform an action such as transferring money to a fraudulent account, or unknowingly downloading malware.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, bitcoin miner, or other code-based malicious entity) that infects an operating system, application or software component. Staff are NOT required to report malware that has been successfully removed by antivirus (AV) software.
Web Attack	Web attacks are executed for a number of purposes including data theft and disseminating malware, and include XSS/Cross Site Scripting, CSRF, SQL Injections, etc. Use this category also for Drupal credentials theft and Drupal website insertion.
Exposure of Credentials	A staff member has leaked valid credentials through a phishing lure, on social media, accidental exposure, or a credentials dump has been reported that includes organization accounts. Also applies when a device is lost or stolen that contains stored credentials.
Unauthorized Access	When an individual or entity gains logical or physical access, without permission, to a network, system, application, data, or other resource. Other steps may follow depending on secondary attacks after access is gained.
Network Attack	An attack on network infrastructure that may include denial of service (DOS), BGP, DNS or ARP cache poisoning, Rogue WiFi hotspot, MiTM devices or methods, reflected DOS, C&C, Service Impersonation, Broken ACLs, etc.
Misconfiguration	When a device or process is configured in a way that allows other types of violations to occur examples include: Unpatched software, vendor updates that include unwanted services turned on by default, use of insecure protocols, etc.
Policy Violation	When an employee violates Acceptable Use Policies or Rules of Behavior. Examples include: Unauthorized use of file sharing software, attachment of non-UCAR-controlled devices to internal UCAR network, accessing or storing pornography, etc.
HIPAA /PHI Exposure	Data loss that includes protected health information (PHI) including health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
Privacy Exposure	Data loss that includes personally identifiable information (PII) as defined by the UCAR Privacy Policy. https://internal.ucar.edu/counsel/privacy-protectionThis category includes unauthorized exposure of personal information covered by the European General Data Protection Regulation (GDPR), the Colorado Protections for Consumer Data Privacy act, or UCAR policy.
CUI /FISMA Exposure	Data loss that includes controlled unclassified information (CUI), ITAR, or data under a FISMA contract constitutes a reportable breach to United States Computer Emergency Readiness Team (US CERT) or Federal Agencies.

Loss of Confidential Information	An incident that involves exfiltration or mishandling of proprietary data, or data that is not considered public open science data, but is not PII, CUI/FISMA or financial data. This may include data about business events or issues, or something that may cause controversy over research or impact public trust.
Financial Fraud Attacks	An incident that involves fraudulent money transfer including fake invoices, fake bank transfers, phony unemployment claims, direct deposit hijacking.