Responsible Disclosure Policy [DRAFT]

Author: Office of Information Technology (OIT)
Version 1.0

Authority:
Duke University Chief Information Officer
Duke University Chief Information Security Officer

Reason for policy

Duke University takes the safety and privacy of our community and data seriously. System users sometimes find security vulnerabilities incidentally during the course of some other activity. Duke is committed to the identification and remediation of security vulnerabilities within systems and networks. This Responsible Disclosure policy addresses the need to identify and report security vulnerabilities within Duke systems and networks.

Policy statement

No individual should set out to attempt to identify a security vulnerability within a Duke system or network without first obtaining permission from the appropriate system owner. Such permission should be obtained prior to engaging in any testing or investigation. Advance notification gives the system owner an opportunity to prepare for any unintended consequences of the security testing or investigation (e.g., unexpected load or non-routine calls being made to the system). The system owner will have discretion in determining whether or not to grant permission.

If a security vulnerability has been identified within a Duke system or network, either through an approved investigation or incidental system use, the individual identifying the security vulnerability must immediately disclose the security vulnerability to the Duke IT Security Office (ITSO). The ITSO will have the responsibility to work with the system or application owner and the identifying party to further investigate and/or resolve the issue through remediation, mitigation or other efforts.

Any identified security vulnerability that has been identified through approved investigating or incidental system use may not be publicly disclosed without explicit permission from Duke, or until after 180 days have passed since the security vulnerability was disclosed to the system owner.

Procedures

Prior to attempting to identify security vulnerabilities within a Duke system:
• To identify the appropriate system owner, please first contact the Duke IT Security Office via email at security@duke.edu.
• Obtain permission from the system owner. This step is not necessary if the system owner is attempting to identify security vulnerabilities in his or her own systems.

When reporting a security vulnerability:

• Contact the Duke IT Security Office via encrypted email at security@duke.edu using our PGP key (available at http://security.duke.edu/itso-pgp-key).
• Include as much information as possible in your report, including a way for the system owner to reproduce the security vulnerability.
• If you are unfamiliar with PGP and encrypting email, then please email us at security@duke.edu and DO NOT include details of the security vulnerability.
• Provide your contact information (email address or phone number).

Publicly disclosing a security vulnerability can put Duke University systems, data and the community at risk. Please do not make your research or findings public or share them with anyone until we have had a chance to investigate and apply a fix.

The Duke University IT Security Office (ITSO) will respond to reports within 3 business days. Responsibly disclosing an issue to the ITSO will allow security vulnerabilities to be addressed as well as recognition provided to those that report the issues.

Scope

All employees, students, affiliates, contractors, consultants, vendors, or other Duke system and network users are covered by this policy.

Enforcement

Violations of this policy may result in loss of Duke system and network usage privileges, administrative sanctions (including termination or expulsion) as outlined in applicable Duke disciplinary procedures, as well as personal civil and/or criminal liability.