

POLICY TITLE:

IT Security Policy

VOLUME, SECTION & NUMBER:

4.2.9

ENTITIES AFFECTED:

Students

Faculty

Staff

Individuals Using KSU Technology Services or Resources

ADMINISTRATIVE AUTHORITY:

Information Technology

Department of Finance & Business Affairs

APPROVED BY:

Kentucky State University Board of Regents

EFFECTIVE DATE:

December 18, 2023

REVISED FROM:

April 2020 Version

B

«

ogy Services

0

Theft or loss of a computing device that may contain Personally Identifiable Information (PII) whether or not such device is owned by KSU

Unauthorized access to data

Computer infected with malware (examples include a worm, virus, Trojan Horse, or botnet)

Reconnaissance activities (such as network or vulnerability scanning, or hacking/penetration testing)

Data Breach

Misuse of Information Resources or Systems

Denial of Service attacks

Security vulnerabilities (such as an un-patched or vulnerable system)

Every user of KSU's Information Technology resources and systems bears responsibility for protecting these technology resources.

KSU will adhere to federal, state laws, rules, regulations, policies, and procedures governing the confidentiality and protection of data.

INCIDENT REPORTING:

Any member of the KSU community who suspects or becomes aware of an Information Security Incident must report the incident immediately by: