

Users are required to protect the confidentiality, integrity, and availability of information technology.

This responsibility includes practicing safe computing at all times when deploying or using BGSU information technology resources. Users are to care for the integrity of technology based information sources they are authorized to access and to ensure that information is shared only with other appropriately authorized users.

BGSU Information Technology Policy – Office of the CIO

SOLID INFO STEWARDSHIP PRACTICES ARE THE BEST SOLUTION TO AVOID INFORMATION SECURITY BREACHES

The public expects universities to be vigilant with sensitive information. An information security breach is costly, damages the reputation of the organization and deters the academic mission of the university. Learn all you can about protecting sensitive information. Get started today!

Visit the Information Security Office website at:

www.bgsu.edu/infosec

INFO STEWARDSHIP



Information Security Office

Information Technology Services
Phone (419) 372-0999



abuse@bgsu.edu
<http://www.bgsu.edu/infosec>

Public Trust: We must act in a way to inspire public confidence in the honesty and integrity of our actions. Any violation of a law, rule, or regulation of the Federal Government, the State of Ohio, the City of Bowling Green, or any other political subdivision where the University transacts its business, violates the public trust and has the potential to discredit the University and impede the furtherance of its mission.

BGSU - CODE OF ETHICS AND
CONDUCT - JUNE 24, 2005

Information Security Office
www.bgsu.edu/infosec

WHAT IS INFO STEWARDSHIP AND WHY IS IT IMPORTANT?

Info Stewardship pertains to the trust placed in those responsible for **managing** information. It is imperative to be vigilant when information is sensitive and consider how it relates to **CIA**:

1. **Confidentiality** - The data is only available to those authorized to have access.
2. **Integrity** – The data is protected from unauthorized modification and destruction.
3. **Availability** – The data and communication are accessible when needed.

Universities contain large amounts of sensitive information. The public trusts and expects universities to safely handle sensitive information.

WHY SHOULD UNIVERSITIES BE CONCERNED?

Universities house large amounts of personal data within a culture of open collaboration. Recent reports suggest criminals attack universities to gather personal information for identity theft because they are easy targets.

It is important to note that universities are the fastest growing group of organizations reporting information security breaches and exposures.

WILL NEW TECHNOLOGY DISCOVERIES FIX THE PROBLEM?

Although new discoveries may be useful, the technologies, standards, and practices currently exist to help minimize the risks. Data stewardship skills along with solid risk management practices are the solution to avoid exposures of sensitive information. Although securing computers and electronic communications add layers of protection, they are not enough to solve the problem. All data handlers need to critically review their daily business practices and improve the human elements of security.

“It was my intention to leave a sizable endowment ... but not any longer.” - university breach victim

STEWARDSHIP PRACTICES HELP PREVENT SENSITIVE INFORMATION EXPOSURES

News stories regarding university breaches provide valuable “lessons learned.” An state university reported exposure revealed the following:

- Donations to the university dropped \$13 million in one financial quarter. Some fundraising programs were eliminated due to the sensitivity of data security issues.
- An initial \$8 million was earmarked to improve security and address other negative publicity incidents.

- It cost \$77,000 to notify the affected students and alumni of the security breach. Here are a few sampled responses:
- ***“You incompetent (expletives).. I will never donate another penny to you.”***
- ***“How could this possibly happen without utter rank incompetence and a carefree attitude toward data security?....”***
- ***“If there is a lawsuit, believe me I will happily join it,”***
- ***“Please stop giving my information to identity thieves....I would give you the rest of my contact information, but I am afraid it would be stolen.”***

THE PUBLIC TRUSTS AND EXPECTS UNIVERSITIES TO SAFELY HANDLE SENSITIVE INFORMATION

The message is simple and the mission is clear. Every university needs to carefully review its data handling processes and make improvements at all levels of the organization. It is the best solution to protect the reputation and mission of the university. The public are counting on us to do the right thing!

Information Security Office

www.bgsu.edu/infosec