“INFOSEC BASIC TRAINING”

By

BU Compliance Services

125 Bay State Road
Boston MA 02215
617-358-8090
compliance@bu.edu

FADE IN:

WELCOME

Slide 1

Welcome to Boston University!
Now that you have successfully set up your University Kerberos account it is important to understand how to keep the BU data you will work with safe and secure.
We all share the same obligation to follow the many different laws and regulations that apply to our University, though our individual responsibilities may be different.

Slide 2

There is a lot of information that the University must manage: student records, financial information, research data, medical records, and business contracts are just some examples.

Slide 3

Your job will determine what data you have access to and what you need to do to protect specific types of data. You will learn more about that from your department. However, there are four basic principles that apply to everyone at BU.

Slide 4

Boston University has developed Data Protection Standards that describe exactly how to collect, access, store, share or destroy specific types of data securely.

Slide 5

Broadly speaking, there are three types of data that require special protection.

Slide 6

Restricted data includes information that Boston University is legally required to safeguard in the most stringent manner.
If the data is breached, the University may be required to notify affected individuals as well as federal or state authorities.

Slide 7

Confidential data is information that, if made available to unauthorized parties, could adversely affect members of our community or the business of Boston University.

Slide 8

Internal data is sensitive information that should not be shared with the public.

Slide 9

Boston University has a variety of programs, applications, and systems that have been evaluated to ensure that the data in those systems is safe and secure. Use those systems for BU data.

Slide 10

Do not store Restricted, Confidential or Internal data in personal cloud applications like Dropbox.

Slide 11

For example, use the University's encrypted email system, SecureMail, for Restricted data or other sensitive information.

Slide 12

Be sure to use BU applications that are appropriate for the type of data you work with.

Slide 13

If you access BU data away from BU, or are using your own electronic devices, make sure your device is secure and you have a secure connection to BU.

Slide 14

Use the University's Virtual Private Network or VPN, if you are working with University data at home or away from your office.

Slide 15

The BU VPN creates a secure "tunnel" between your computer and the campus network.

Slide 16

You can use your personal computer, tablet or phone as long as it meets the University's Minimum Security Standards.

Slide 17

Report anything suspicious.
If you are unsure, it is better to ask.
You have several ways to contact the Information Services and Technology Help Center.
The IS&T Help Center is staffed seven days a week.

Slide 18

If you receive a suspicious email, forward the message to abuse @ bu.edu and then delete it.

Slide 19

If you suspect that your Kerberos password has been compromised, reset the password immediately then report what happened to the IS&T Help Center.

Slide 20

If you suspect your computer has a virus or other malware, call the IS&T Help Center at 617 353 HELP.

Slide 21

Report any suspected data breach immediately.
A data breach includes any unauthorized access or use of sensitive information that creates a substantial risk of identity theft or other harm.

Slide 22

If you have questions or would like to give us feedback, look for us on the web.

Thank you for taking the time to listen.
Now you are officially part of the BU community!

THE END