OFFICE SECURITY AND DATA PROTECTION

Data protection is based on the following key principles that should guide the daily decisions on what data is accessed and how it is held.

ASK QUESTIONS
about your data

- What data is touched (SS Numbers, other personal info).
- Where is the data stored? (Laptop, cloud, disc, etc.)
- Is an email necessary? Is information ever emailed or transfered?

TAKE STOCK

- Understand what personal information your department has and where is it stored.
- Take a mental inventory of laptops, flash drives, external drives, online repositories, email.
- How is this data received and does your department forward to other individuals?
- Who sends data and is it sensitive
- What methods are used for transferring data, and how should it be received if it includes private or sensitive data?
- Printers & Faxs - Will information be sent to these devices? Where are they located?

ACCESS
to information

- Who should have access to the information?
  Staff, faculty, students or student workers, DCCs
- Where can the information be viewed?
  Public computer, shared computer
  Home computer
- Password Management: strong and private.
  Do not allow another individual to work with your credentials.

Knowledge + Action = Power

For more information on data protection and office security go to https://security.arizona.edu.

THE UNIVERSITY OF ARIZONA
Information Security

OFFICE SECURITY AND DATA PROTECTION

DATA CONSIDERATIONS

When accessing the UAccess enterprise systems, review:

- What information is being gathered
- What business need is it fullfilling
- How long do you need it for

FERPA

The Family Educational Rights and Privary Act. All education data holders must act responsibly and be held accountable for safefuarding students' peronally identifiable information (PII) from education records. Assess where this data is stored and review encryption standards for additional protections.

GDPR regulations

GDPR is designed to modernize laws and boost the rights of individuals, giving more protection over personal information. Data handling must follow the GDPR guidelines for:

- Student employees from the EU
- Student employees traveling to the EU
- Information or contractors located in the EU

PROTECT IT

If you don't need it, don't seek it. If you no longer need it, delete it.

- Physical Security: Keep papers, files, discs in locked area.
- Lock computers when not using and keep in secure locations
- Shorten or truncate SS# or CC info, and do not keep on file
- Check default settings on software
- Follow the retention and disposal policy guidelines for items no longer needed.
- Shred Paper Documents no longer needed and 'Wipe" old computers

Refer to the UA Data Classification and Handling Standard at security.arizona.edu/data

For more information on data protection and office security, go to https://security.arizona.edu.

THE UNIVERSITY OF ARIZONA
Information Security