OVERVIEW

- Our responsibilities
- What the data tells us
- The CSU response
- Protected data
- Responsible Use Policy
- Malware
- Phishing
to make sure that none of the information we collect becomes available to criminals;

to make sure that private information is kept private;

to make sure that our systems maintain integrity - that is to say that grades and academic work is protected from tampering or disclosure;

to make sure that state property isn’t used improperly.
Incidents by Business Type - All Time

- Gov - 21%
- Edu - 25%
- Med - 12%
- Biz - 42%
All types of information security breaches since 2003 (from datalossdb.org)
Data breaches 2005-2008 from educational institutions. Information gathered from http://datalossdb.org
CSU-Wide security policies and standards apply as a minimum baseline to all campus.

Campuses implement with local procedures and standards.
Information Security Roles and Responsibilities
Risk Management
Acceptable Use
Personnel Security
Privacy
Security Awareness and Training
Third Party Services Security
Information Technology Security
Configuration Management and Change Control

Access Control
Asset Management
Management of Information Systems
Information Security Incident Management
Physical Security
Business Continuity and Disaster Recovery
Legal and Regulatory Compliance
"PROTECTED" DATA IS...

...confidential data exempt from public disclosure the unauthorized access to which could result in severe damage to the CSU.

Examples include but are not limited to:
- Username along with password or PIN
- Name combined with SSN, Payment Card number, Driver’s License
- DOB + last four of SSN
- Bank account or Credit Card + access code
- Health insurance information
- Medical records
Requires a level of “reasonable cause” in order to access individual’s files/email.

Advises that private data may be exposed to system administrators.

Acknowledges “incidental personal use” of state equipment.

Prohibits sending of unencrypted “protected” data.

Prohibits misrepresentation of identity.

Must secure your remote system if it accesses the campus!
Malware: software designed to infiltrate or damage a computer system without the owner’s informed consent.

Most malware now has a profit motive - either advertising or criminal activities.

It *is* possible to infect a campus computer.

Infected computers may require a wipe and reload.
Phishing is the attempt to get you to send in your password or credit card or similar credential.

These are often sophisticated messages that pretend to be from your bank, or from ebay or from us.

You should never respond to one of these with any information. Never send your credit card or your password.

Remember: we will never ask you to send your password over email.
CSU-Wide policies and standards will be implemented on our campus.
You will be notified and asked to sign a responsible use policy and/or confidentiality agreement depending on what data you access.
We will be taking a closer look when we store protected data or create servers and this also applies to grant-funded efforts.
There will be CSU-wide security awareness training that everyone will complete.
QUESTIONS?