InterMountain EDUCATION SERVICE DISTRICT

2001 SW Nye Avenue
Pendleton, Oregon 97801
main 541.276.6616
www.imesd.k12.or.us

Core Principles of Information Security (CIA Triad)

- Confidentiality – *Security is in place to ensure data is only accessible by those authorized.*
- Integrity – *Ensure data presented is reliable and absent of errors (corrupted, damaged, destroyed, or altered).*
- Availability – *Reliable data is readily available upon request by those authorized.*

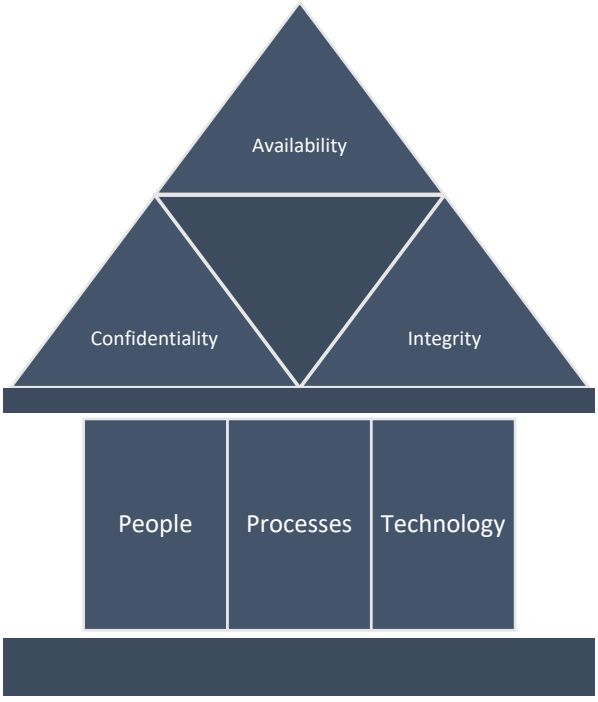
Program for Information Security

- Governance, Risk, and Compliance (GRC) Program
  - Governance – *Management of people, process, and technology. Ensures that organization objectives are achieved by **evaluating** stakeholder needs, conditions, and options; setting **direction** through prioritization and decision making; and **monitoring** performance, compliance and progress against agreed direction and objectives (EDM).*
  - Risk – *Continually identify, assess, and reduce IT-related risk within levels of tolerance set by the organization.*
  - Compliance – *Ensure the organization is compliant with all applicable external requirements. (FERPA, CIPA, COPPA, HIPPA, GDPR, Oregon Student Data Privacy, public records, etc.)*

Information Security Notes

- Cybersecurity is a specific component of information security.
- Guaranteed security does not exist. Information security is a constant cat and mouse situation between the organization and nefarious agents trying to outsmart one another.
- Information security must be a balance between security and business operations. Decisions regarding information security must be informed risk analysis based.

Three Pillars of the CIA Triad



People

- Ensure everyone in the organization is aware of their role in preventing and reducing information security threats.
- Ensure technical staff are up to date with the latest skills and qualifications to enable the implementation of appropriate controls, technologies, and practices.

Processes

- Ensure the organization's policies and processes define activities and roles that mitigate risks to data.

Technology

- Monitor and ensure the appropriate technologies and technological controls are in place.
- Perform risk analyses to determine the need for improvements or adjustments.