**1. What is information security?**

Information security is the practice of protecting information and information systems from unauthorized disclosure, modification, and destruction. It encompasses the security of all IT resources, including both University information and the IT devices that access, process, store, or transmit it.

**2. What is Secure UD?**

Secure UD is the University's comprehensive, community-oriented information security initiative. It empowers and equips the University community to make sound security and risk decisions in their personal and professional lives.

**3. What is University information?**

University information is the set of information that the University owns or for which the University is accountable. Included in this definition are all data relevant to or that supports the administration and missions (teaching, research, and service) of the University.

**4. What is an IT device?**

An IT device is any device that is used to access, process, store, or transmit University information and that uses the University's IT infrastructure, including the University network. Examples of IT devices include desktop computers, laptop computers, smartphones, tablets, network devices, and printers.

**5. What are IT resources?**

IT resources are the full set of University-owned or -controlled IT devices and data involved in the accessing, processing, storage, and transmisison of information. IT resources include both University information and IT devices.

**6. What is confidentiality?**

[**Confidentiality**](https://www1.udel.edu/security/data/confidentiality.html) is the preservation of authorized restrictions on University information access and disclosure, including means for protecting personal privacy and proprietary information.

Confidentiality has to do with the privacy of information, including authorizations to view, share, and use it. Information with low confidentiality concerns may be considered "public" or otherwise not threatening if exposed beyond its intended audience. Information with high confidentiality concerns is considered secret and must be kept confidential to prevent identity theft, compromise of accounts and systems, legal or reputational damage, and other severe consequences.

**7. What is integrity?**

[**Integrity**](https://www1.udel.edu/security/data/integrity.html) is the protection against improper modification or destruction of University information. It includes non-repudiation and authenticity.

Integrity has to do with the accuracy of information, including its authenticity and trustworthiness. Information with low integrity concerns may be considered unimportant to precise University activities or not necessary to vigorously check for errors. Information with high integrity concerns is considered critical and must be accurate in order to prevent negative impact on University activities.

Integrity concerns—along with availability concerns—contribute to data's [**criticality**](https://www1.udel.edu/security/data/criticality.html).

**8. What is availability?**

[**Availability**](https://www1.udel.edu/security/data/availability.html) is the timeliness and reliability of access to and use of University information.

Availability has to do with the accessibility and continuity of information. Information with low availability concerns may be considered supplementary rather than necessary. Information with high availability concerns is considered critical and must be accessible in order to prevent negative impact on University activities.

Availability concerns—along with integrity concerns—contribute to data's [**criticality**](https://www1.udel.edu/security/data/criticality.html).

**9. What is criticality?**

[**Criticality**](https://www1.udel.edu/security/data/criticality.html) is the importance of data availability and integrity to the business continuity and operational effectiveness of the University.

Criticality is a reflection of data's integrity and availability concerns. Data's criticality is the higher of its integrity and availability concerns. For example, data with high integrity concerns but moderate availability concerns would have a high criticality.

There are three levels of criticality:

1. Non-critical
2. Critical
3. Mission critical

**10. Isn't information security an IT issue?**

Information security is an organizational issue, not exclusively an IT issue. IT provides security to central systems and the University network. However, much of the risk to IT resources can only be managed within units' day-to-day operations. We all share responsibility for properly managing the University's IT resources, including University information and IT devices.

Units have significant autonomy to fulfill their operational missions. Each unit has a responsibility to manage its own security posture just like each individual has a responsibility for his or her own actions. Security is a balance between the need for information security and the need for information use.