

Search Old Dominion University and the Web for examples of issue-specific security policies.

1. What types of policies can you find?
 - a. There are many types of policies that cover various types of issues a couple of examples I got from ODU are Closure of the University Due to Inclement Weather & Emergencies, Policy on University Audit Response Procedures, Electronic Mail Policy for Official University Business, and Information Technology Access Control.

2. Using the format provided in this module, draft a simple issue-specific policy that outlines fair and responsible use of computers at your university based on its rules and regulations. Provide a side by side view your yours and the university's policy. clearly highlight the differences. Does it contain all the elements listed in the text?

ISSP based on the book

1. Statement of policy
 - a. Scope and applicability- it applies to all computers connected to the ODU network.
 - b. Definition of technology addressed- any device capable of computing and communications over the network needs to follow these rules.
 - c. Responsibilities- this responsibility falls on the users to follow the rules and network analysis to catch any unauthorized uses.
2. Authorized access and usage of equipment
 - a. User access- any device that has registered to the network by a valid university-authorized user.
 - b. Fair and responsible use- the devices are allowed to access the network as long as it does not violate the rules.
 - c. Protection of privacy- only the university will be able to view what goes across its network and may be stored for future investigations.
3. Prohibited use of equipment
 - a. Disruptive use or misuse- all devices should be respectful of the network and not intentionally create problems.
 - b. Criminal use- the network should not be used for criminal attacks or uses.
4. Systems management
 - a. Network monitoring- the university has the right to monitor all of the traffic and log it for future investigations.
 - b. Physical security- The traffic data is stored in secure locations that only authorized personnel can access.
5. Violations of policy
 - a. Procedures for reporting violations- an investigation will be held when a suspected violation takes place.
 - b. Penalties for violations- the university holds the right to terminate a user's complete access to the network.
6. Policy review and modification

- a. Scheduled review of policy procedures for modification- This is reviewed yearly and changes are made.
- 7. Limitations of liability
 - a. Statements of liability- use of the network is at the users' discretion and all actions taken are of their own volition.
 - b. Other disclaimers as needed

ISSP from ODU [3500: Policy on the Use of Information Technology Resources](#)

There are many differences between the ones created from the book and what the university has posted online. The one the university has made is broken into multiple policies, because they have the “acceptable use” in a different document. They are structured in a slightly different way, the book has Statement of policy, Authorized access and usage of equipment, Prohibited use of equipment, Systems management, Violations of policy, Policy review and modification, and Limitations of liability. While the university has PURPOSE, AUTHORITY, DEFINITIONS, SCOPE, POLICY STATEMENT, PROCEDURES, RECORDS RETENTION, RESPONSIBLE OFFICER, and RELATED INFORMATION. While they have some similar sections like the policy statements they have a couple of different sections like procedures, records retention, and related information.

I think that the university has all of the same elements of the one in the book. However, the university’s policy seems much more compact and well-refined into more understandable documents.