1. **Overview/need for the policy**:

The goal of the policy should be such it attempts to protect the computer infrastructure used by the students, employees and the other staff who do direct business (vendors) with the Sunshine State University. It could have a huge impact on the user’s privacy as many users may not adhere to the guidelines or policies of the organization. The need for the policy is to design a policy which the Sunshine state university students and employees will be able to use the computer equipment and storage.

1. **Scope**:

Everyone who comes under the hood of Sunshine State University will be applied the policy stated above. I mean the faculty, students, staff, and other people who are connected to the University are covered by this policy. It is applied for all electronic devices used for compute, storage and networking. They can be under a third-party lease. But putting all the policies in a single document is also not recommended, so the scope depends upon the type of the policy.

1. Statement of Policy:

This part of the policy defines that every user in the university must comply to the guidelines of the university. They must use the cloud services which adhere to the acts like PPM 10-1, HIPAA, FERPA or the cloud services which are approved by the IT support team of the University.

The use of the information correctly or misuse should be documented in compliance with the all the acts. The information access must be restricted to the individuals who have the authority.

The internal audit control team should be given the access to check the systems and the networks in the organization at any time to ensure everything is in compliance with the law.

Now-a-days everyone has uses more than two devices. These are connected to the University’s network and the multi-factor authentication should be enabled in trusting the certificate of the device. This should help in improving the security of the laptops, mobiles, and other storages.

The spam or malware attachments are becoming more common these days. They are coming as the attachments or the links in the emails. These links or attachments should be scanned in before hand by the internal security team and flag them as safe or unsafe. This should protect many of the untrained individuals.

All the employees and staff should not involve in any kind of breach or the violations of the rights or rules of the government or security body. Accessing or misusing the access to the database or the storage will also lead to huge felony. Trying to misuse the University email for illegal activities or anti-social activities may also cause the imprisonment. Network intercepting or illegal scraping of the website information by introducing bots is also not allowed. This causes the slowdown or make the website unavailable for the normal users.

The policy is used in protecting the proprietary information of the University like Research in health and technology, University’s anthem, or symbols, and all the information regarding the funds of received from the government.

1. Enforcement:

This policy ends with this section. This generally deals with all the penalties with respect to acts and it includes what “might” happen to the users or the organizations if they do not adhere to the acts rather than ‘must’ or ‘should’.

It specifies the confidentiality and the use of the data. For example, Sensitive Data of the Institution is only limited to the people who has access. The research data or the personal information of the members of the university. In this case, almost all the sensitive information is stored on-premises or in the central storage without having replicas because of the security issues. It follows the same for the other kind of data. The penalties for violating any kinds of rules or acts may be followed with a felony or huge monetary fine of up to $ 1,000,000.

There are different enforcements for different kinds of information with the different penalties.

Exceptions to this policy can also be approved by ISO under ESCC.