**Incident Response Plan**

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}

Standard: US-CERT, CSIRT, VERIS

**Mission, Stratégies and goals:**

* What are we trying to protect
* What are threats
* How do we detect the threats
* How do we respond to threats

**Incident response approach:**

1. **Preparation**
2. **Identification - VERIS**

* **Actions [Hacking, Social, Malware, Misuse]**
* **Actors [Internal, External, Partner]**
* **Asset [Server, Network, User Device]**
* **Attribute [Confidentiality, Integrity, Availability]**

1. **Analysis**
2. **Containment**
3. **Eradication and Recovery**
4. **Lessons Learned**
5. **Reporting**

**Approval from senior management**

**Communication**

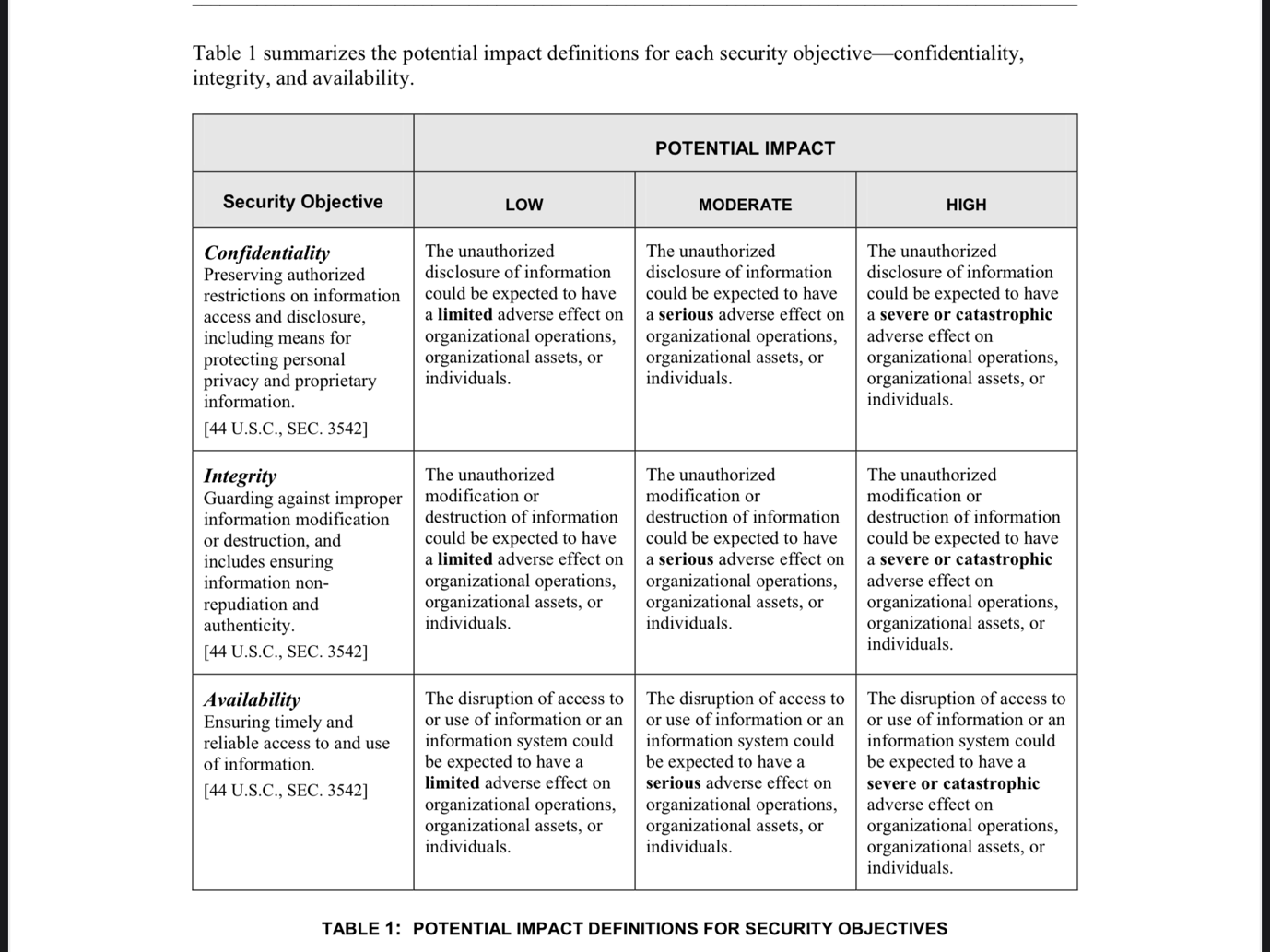
**Metrics**

**Review**

**Organisation missions**

**Appendix**

**FIPS-199**

****