**CYBERSECURITY FRAMEWORK**

**4.4 CONTROLS**

These controls are based on ISO/IEC 27001: 2022. By following these standards, our university can reduce the risk of unauthorized access, disclosure, modification, or destruction of its information assets. It will improve the information security posture of our university and also reduce the risk of data breaches. As a result the name and reputation of our university will enhance.

* **TECHNICAL CONTROLS**

1. **User end point devices.** Information stored on, processed by or accessible via user end point devices shall be protected**.*[ISO 27001: 2022 (8.1)]***
2. **Privileged access rights**. The allocation and use of privileged access rights shall be restricted and managed***.[ISO 27001: 2022 (8.2)]***
3. **Information access restriction**. Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control***. (8.3)***
4. **Access to source code**. Read and write access to source code, development tools and software libraries shall be appropriately managed***. (8.4)***
5. **Information deletion.** Information stored in information systems, devices or in any other storage media shall be deleted when no longer required***. (8.10)***
6. **Data leakage prevention**. Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information***. (8.12)***
7. **Information backup.** Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup. ***(8.13)***
8. **Monitoring activities**. Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents***. (8.16)***
9. **Web filtering.** Access to external websites shall be managed to reduce exposure to malicious content***. (8.23)***
10. **Networks security**. Networks and network devices shall be secured, managed and controlled to protect information in systems and applications***. (8.20)***

* **ADMINISTRATIVE CONTROLS**

1. **Classification of information** Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements. ***(5.12)***
2. **Labelling of information** An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization***. (5.13)***
3. **Access control** Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirement***. (5.15)***
4. **Identity management** The full life cycle of identities shall be managed***. (5.16)***
5. **Protection of records** Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release***.(5.33)***
6. **Physical security perimeters** Security perimeters shall be defined and used to protect areas that contain information and other associated assets. ***(7.1)***
7. **Physical entry** Secure areas shall be protected by appropriate entry controls and access points***. (7.2)***
8. **Securing offices, rooms and facilities** Physical security for offices, rooms and facilities shall be designed and implemented***. (7.3)***
9. **Physical security monitoring** Premises shall be continuously monitored for unauthorized physical access***. (7.4)***
10. **Storage media** Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization’s classification scheme and handling requirements***. (7.10)***