University of North Texas Data Privacy Protections

1. **University Policies and Standards**. University policies and standards are in place to comply with state and federal requirements for protecting the privacy of information.

2. **Information Security and Privacy Program**. The information security program operates to ensure the confidentiality, integrity, and availability of information and information resources. An information privacy function is in place to support the protection of Personal Identifying Information (PII) and confidential data.

3. **Least Privilege**. UNT has adopted the principle of least privilege which limits access to information and technology to only that which is needed in order to conduct business.

4. **Security Roles and Responsibilities for Protecting Data**. University employees are assigned roles and responsibilities for protecting data based on their security role in the University.

5. **Access Control**. Access to PII and confidential data is limited to the individuals that are authorized by information owners to view or use the information.

6. **Appropriate Use**. Individuals are required to use information in a manner that does not compromise its security or privacy.

7. **Data Collection**. The University limits the collection, use, processing, and disclosure of PII to that which serves to meet its function and purpose.

8. **Data Protection**. Data are protected in accordance with their assigned information category. PII and confidential data receive the highest level of protection in information systems.

9. **Data Retention**. University policies for records management identify data retention practices.

10. **Training**. Security and privacy awareness training is mandatory for individuals that access PII and confidential data.

11. **Security Risk Management**. Risk management procedures are in place to assess the weaknesses and vulnerabilities associated with handling PII and managing information technology.

12. **Security Incidents**. Users have the ability to report suspected or confirmed security violations immediately to the information security team, IT helpdesks, and their supervisors. Security and privacy incidents are investigated immediately.

Published: 10/29/2020
Next Review Date: 10/29/2021

13. **Cloud Services Security**. Cloud services are assessed to ensure that service providers are capable of protecting PII and confidential data prior to the release of data for information processing purposes.

14. **Service Providers**. Service providers must acknowledge their responsibilities for complying with institution policies and standards prior to receiving access to institutional information assets. Service providers may not share confidential information with third-parties without the express permission of the University.

15. **Contracts and Agreements**. Contracts are reviewed to ensure that non-disclosure agreements are in place between the University and service providers, and to ensure that the disposition of confidential data is handled appropriately to ensure its protection.

16. **Technology Controls**. Technology controls are in place to protect the privacy and security of information. Technology is regularly assessed to ensure compliance with a robust set of data protection standards that are based on state and federal data protection laws.

Published: 10/29/2020
Next Review Date: 10/29/2021

References:

- UNT Information Security Policy 14.002
- UNT System Information Security Handbook
- UNT Computer Use Policy 14.003
- UNT Privacy Policy 05.046
- UNT FERPA Policy 07.018
- UNT Ethics Policy 05.015

Published: 10/29/2020
Next Review Date: 10/29/2021