External Sharing Policy

Policy Information

ISSUING OFFICE

Information Services

POLICY

Sharing Liberty University data outside of Liberty University should be controlled and monitored to ensure that unauthorized leaks in such data, including data breaches, do not occur.

SCOPE

This policy applies to all Liberty University faculty and staff, including student workers (also collectively referred to herein as, ?employees?), regardless of location or device being used. This policy also applies to University students but only to the extent that they handle any internal, sensitive, or highly sensitive data, as those terms are defined in the Data Classification Policy. Students sharing data as necessary to complete coursework is not covered by this policy. Other University policies may also apply to conduct that falls within the scope of this policy.

PURPOSE

The purpose of this policy is to help prevent leaks and breaches of Liberty University data to unauthorized third-parties by adopting standards for external data sharing by Liberty University employees. Sharing Liberty University data outside of Liberty University without first performing the necessary precautions can have severe consequences for the University, including causing irreparable harm to the University?s departments, its students, its employees and its mission. Knowing and understanding the boundaries for external data sharing, especially sensitive and highly sensitive data can help prevent (and mitigate) leaks and breaches of data caused by inappropriate data sharing.

Before sharing data with third-parties or unauthorized internal parties, the following considerations should be kept in mind:

- Confidential data that is shared with, or that is unprotected from, unauthorized third-parties can lead to prosecution in certain cases.
- The inappropriate and possibly unlawful release of information may result in legal liability and/or prosecution.
- Release of sensitive or highly sensitive data, even if inadvertent, to other parts of the University without authorization may lead to an unauthorized sharing of that data with third-parties that can have severe consequences for the University.
- The recipient of the data, the recipient?s systems, and the networks on which data is shared (especially if not sufficiently secure and protected) may compromise the confidentiality of sensitive and highly sensitive documents and data, thereby becoming a security threat which could be exploited to cause harm.

STANDARDS

All applicable laws and regulations governing data must be followed by the University and its employees. Data may be shared in compliance with the law, including to comply with lawfully-issued subpoenas and court orders, or as permitted by the Family Educational Rights and Privacy Act of 1974 (FERPA), in accordance with University policies and procedures. Contact the Legal Affairs Office prior to sharing data in legal matters, such as subpoenas and court orders.

Data and information must only be shared with individuals or businesses that have the correct and appropriate access level for the data being shared.[1]

Instructing employees about the applicable laws and regulations governing data use, as well as about the best practices for storing and sharing data, should include details about legal and University consequences for inappropriately sharing and disclosing data, both internally and externally.[2]

Employee data may only be shared with individuals and businesses specifically authorized to receive the data. Authorization must be obtained by the University prior to sharing the data.[3]

Attaching data files to an email must only be permitted after confirming the classification of the data being sent and verifying the recipient has the authority to receive the data.[4]

Sensitive and highly sensitive data may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured, (e.g. by using encryption techniques), as mentioned in the Remote Access Policy.[5]

Only authorized persons are permitted to share or knowingly access sensitive or highly sensitive data and that data may only be used for authorized University purposes.[6]

Sensitive or highly sensitive data may only be faxed when more secure methods of transmission are not feasible under the circumstances. Both the possessor of the data and the intended recipient must authorize the transmission beforehand.[7]

Any leaks or breaches of data must be reported to the Legal Affairs Office as soon as possible.

Data Sharing Security Standards for Vendors and Affiliates

In addition to the above standards, which standards generally apply to University systems, it is also important to have certain assurances regarding the data and network security of vendors? and affiliates? systems prior to sharing data. Prior to sharing data or reports with vendors and affiliates, not only must the intended recipient be pre-authorized to receive such data, but the data use procedures and Information Security measures of the third party, must be reviewed and approved by the University to continue to assure the confidentiality and integrity of the data being shared before the data is shared with the third party.[8]

Use of Collaborative Software

Collaborative software that will be used in part for sharing with external individuals or businesses should, where practical, keep external sharing settings on, provided the users maintain the standards outlined in this policy with respect to sensitive and highly sensitive information. Information protection software should, where practical, be set to remove any personally-identifiable information (PII) and/or to block that information from being sent out.

Users of collaborative software should be trained on the correct method of data sharing (such as how to share a document versus sharing a site) to avoid inadvertently giving unauthorized access to sensitive or highly sensitive data.

VIOLATIONS

Violation of this policy may subject the employee to discipline up to and including immediate termination without pay and/or administrative withdrawal from the University, as well as monetary fines and/or damages for financial loss. Violations of this policy may also violate other University policies and/or federal or state laws.

DEFINITIONS

Data - ?A subset of information in an electronic format that allows it to be retrieved or transmitted.? (Data Classification Policy)

Information Security - ?Protection of information to ensure confidentiality, integrity, and availability.? (PCI DSS Glossary, April 2018)

PII - Personally Identifiable Information

Sensitive Information - ?Information which may cause financial or reputational damage to the university, its students and/or employees if mishandled. Sensitive information is only to be consumed by audiences that have been made aware of the data content.? (Data Classification Policy)

Sharing - For the purpose of this policy, ?sharing? data means taking any action that results in providing, disclosing, releasing, sharing, sending, transmitting, creating an opportunity to view, or otherwise giving another individual access to data, or taking any action that is reasonably likely to result in another individual obtaining access to data.

Highly Sensitive Information - ?Information that should be handled only by applicable departments or individuals. Inappropriate use of highly sensitive information could cause substantial and immediate harm to the image or financials of the University, its students and/or employees.? (Data Classification Policy)

RELATED POLICIES

IS020121 Acceptable Use Policy

IS010108 Data Classification Policy

IS010109 Privacy Policy

IS030103 Remote Access Policy

REFERENCES

ISO/IEC 27002:2013 (More information available upon request)

07.02.02 Information security awareness, education, and training

08.02.01 Classification of information

09.01.01 Access control

10.01.02 Key management

13.02.01 Information transfer policies and procedures

14.01.02 Securing application services on public networks

18.02.04 Privacy and protection of personally identifiable information

NIST 800-171 More Information here

3.1.3 Access control

---

[1] . NIST 800-171 3.1.3; ISO Policy 100303

[2] . ISO 08.02.01, 18.02.04 (ISO Policy 030802)

[3] . ISO 07.02.02 (ISO Policy 100205)

[4] . ISO 14.01.02, 10.01.02 (ISO Policy 030303)

[5] . ISO 13.02.01 (ISO Policy 030501)

[6] . ISO 9.01.01 (ISO Policy 030516)

[7] . ISO 13.02.01 (ISO Policy 050203)

[8] . ISO 13.02.01 (ISO Policies 030803, 030807)