Institutional Engagement - Compliance Requirements

Updated:	10/1/2022	initials of Completer: ALM						
Compliance Requirement	**Compliance Organization**	**Description of Requirement**	**Responsible Department**	**Responsible Party**	**Frequency**	**Last Date Completed**	**Consequence/ Penalty**	**Month**
Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)	Federal Trade Commission	Prohibits the inclusion of deceptive or misleading information and subject headings, requires identifying information such as a return address in email messages, and prohibits sending emails to a recipient after an explicit response that the recipient does not want to continue receiving the messages. Resources: Higher Education Compliance Alliance (http://www.higheredcompliance.org) and the Legal Information Institute (https://www.law.cornell.edu/uscode)	IE	Vice President for IE	Ongoing	N/A	Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000.	Ongoing
Freedom of Information Act	Department of Justice	Provides a process by which every person may request access to a public college or university's records or information. Resources: Higher Education Compliance Alliance (http://www.higheredcompliance.org) and the Legal Information Institute (https://www.law.cornell.edu/uscode)	IE	Vice President for IE	Ongoing	N/A	Legal action and reputational vulnerability.	Ongoing

Institutional Engagement - Compliance Requirements

Compliance Requirement	Compliance Organization	Description of Requirement	Responsible Department	Responsible Party	Frequency	Last Date Completed	Consequence/ Penalty	Month
GeneralData Protection Regulation (GDPR)	European Union	The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. Controllers of personal data must put in place appropriate technical and organizational measures to implement the data protection principles. Business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate), and use the highest-possible privacy settings by default, so that the datasets are not publicly available without explicit, informed consent, and cannot be used to identify a subject without additional information (which must be stored separately). The data subject has the right to revoke this consent at any time. A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the EEA. Data subjects have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy. In some cases, violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.	IE	Vice President for IE	Ongoing	N/A	Legal action and reputational vulnerability.	Ongoing
Gramm Leach Bliley Act (GLBA)	Federal Trade Commission	Governs the collection, disclosure, and protection of consumers' personal information and personally identifiable information (defined as names, addresses and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers). Requires institutions that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information-sharing practices to their customers and to safeguard sensitive data. Resources: Federal Trade Commission website https://www.ftc.gov/tips-advice/business-center/guidance/safeguarding-customers-personal-information-requirement; Higher Education Compliance Alliance (http://www.higheredcompliance.org); and the Legal Information Institute (https://www.law.cornell.edu/uscode)	All of RISD's Departments; IE related to constituent engagement (individual and corporate/foundation), online giving and e-commerce.	Vice President for IE	Ongoing	N/A	Legal action and reputational vulnerability (data breach).	Ongoing

Institutional Engagement - Compliance Requirements

Compliance Requirement	Compliance Organization	Description of Requirement	Responsible Department	Responsible Party	Frequency	Last Date Completed	Consequence/ Penalty	Month
Higher Education Opportunity Act (HEA)	Department of Education	Institutions of higher education are required to submit a disclosure report for gifts and contracts of $250,000 or more with a foreign source to the Department of Education. Resources: Higher Education Compliance Alliance (http://www.higheredcompliance.org) and the Legal Information Institute (https://www.law.cornell.edu/uscode)	IE	Vice President for IE	July 31 and January 31 annually when qualifying gifts are received	IE is currently preparing a report of foreign gifts from the past 5 years	If an institution fails to comply with the reporting requirement in a timely manner the Secretary may	July/ January
Internal Revenue Code: Substantiation and Disclosure Provisions	Internal Revenue Service	Substantiation and disclosure provisions apply to contributions made to tax-exempt organizations after December 31, 1993. For charitable contributions of $250 or more, the donor must receive a contemporaneous written acknowledgment from the organization of the gift and indicate whether goods or services were received in exchange for the gift. The acknowledgment should note the amount of any cash contribution and, if the donation is in the form of property, the acknowledgment must describe, but need not value, the property. Valuation of the property is the responsibility of the donor. Institutions must also provide a written disclosure statement to the donor(s) who make payments described as quid pro quo contributions in excess of $75. Resources: Higher Education Compliance Alliance (http://www.higheredcompliance.org) and the Legal Information Institute (https://www.law.cornell.edu/uscode)	IE	Vice President for IE	Ongoing	Daily	If the IRS decides that a nonprofit has failed to comply with applicable tax laws and regulations, the agency has the power to impose monetary penalties, excise taxes, and even revoke a nonprofit's tax exemption, in extreme cases. Excise taxes may	Ongoing
Payment Card Industry (PCI) Data Security Standards	No federal legislation. Governed by State law and guided by the PCI Security Standards Council,	The PCI Security Standards Council (SSC) defines "cardholder data" as the full Primary Account Number (PAN) or the full PAN along with any of the following elements: Cardholder Name, Expirations Date or Service Code. Resources: PCI Security Council www.pcisecuritystandards.org and State of Rhode Island www.ri.gov/policies/security	IE	Vice President for IE	Ongoing	N/A	The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per	Ongoing
Philanthropy Protection Act of 1995	Federal Trade Commission	Requires institutions of higher education to provide a disclosure statement to all annuitants in a Gift Annuity Fund and **also to provide the same to all prospective donors at the time of solicitation**, using a letter or pamphlet format. Resources: Higher Education Compliance Alliance (http://www.higheredcompliance.org) and the Legal Information Institute (https://www.law.cornell.edu/uscode)	IE	Vice President for IE and Controller	Ongoing		Criminal and civil penalties. Reputational vulnerability.	Ongoing

Institutional Engagement - Compliance Requirements

Compliance Requirement	Compliance Organization	Description of Requirement	Responsible Department	Responsible Party	Frequency	Last Date Completed	Consequence/ Penalty	Month
Telemarketing and Consumer Fraud and Abuse Prevention Act	Federal Trade Commission and guided by the National Committee on Planned Giving (NCPG) and the American Council on Gift Annuities (ACGA)	As tax-exempt nonprofits, institutions of higher education are exempt from the Do-Not-Call-Registry, but may not call any residential telephone subscriber before 8 a.m. or after 9 p.m., local time at the called party's location. Resources: Higher Education Compliance Alliance (http://www.higheredcompliance.org) and the Legal Information Institute (https://www.law.cornell.edu/uscode)	IE	Vice President for IE	Ongoing	N/A	State and Federal fines ranging up to $11,000 per violation. Consumers continue to have the authority to bring a civil action against the violating party. Reputational vulnerability.	Ongoing