ACCEPTABLE USE OF TECHNOLOGY POLICY

1. **Purpose**
   To ensure Bay Path University (BP) and all BP Users are responsible for proper use of information and protected from illegal and/or harmful actions that result from inappropriate use of BP Systems.
2. **Definitions**
   - BP users: All University employees, faculty, adjunct faculty, and students, in addition to all contractors, consultants, temporary workers, per diem, volunteers, visitors, and student workers that access BP Systems.
   - BP systems: All equipment and data owned by BP, which includes: individual computing and storage devices (desktop, laptop, tablet, printer, flash drive, etc) and any data contained on them; as well as enterprise computing resources (e.g. Jenzabar, internet access, e-mail, file shares, software, servers, networks, phone systems, system accounts).
   - BP data: All information stored, processed, or transmitted through BP systems and used by the BP users for academic or administrative operations. Such data is owned by the University and not the user.
   - Confidential data: Social security number, ID number, student educational records as defined by FERPA (including grades), financial data, account numbers, bills, personnel files, passwords, and any other information labeled as confidential by BP users. BP will take reasonable steps to protect personal information as permitted by law.
3. **Responsibilities of BP Users**
   a. Use that is consistent with the BP mission and policies;
   b. Use in an ethical and lawful manner;
   c. Use which consistently protects the confidentiality, integrity, and availability of BP data:
      i. Ensure data are accurate, prevent mishandling;
      ii. Ensure access to data are limited to the needs of a job function;
      iii. Ensure that data are available for appropriate University personnel;
4. **Privacy & Monitoring**
   All University owned property and the data therein, whether stored electronically, on paper, or in any other form, are subject to review at the discretion of the University. Portions of the IT infrastructure include automatic and manual monitoring and recording systems that are used for reasons that include, but are not limited to, security, performance, backup, and troubleshooting. The University reserves the right at any time to monitor and access any data, including the contents of any University computer or University communications, for any legitimate business reason.
5. **Personal Use**
   The University recognizes that limited personal use of BP systems may be necessary from time to time to attend to personal matters that cannot be handled outside work/school hours. Limited personal use of BP Systems must not interfere with or disrupt the work of the unit or other University business or educational activities nor unduly burden BP Systems such that they are not available for business and educational use. Bay Path systems may not be used for the purpose of a personal business (for profit or not for profit) or for any political activities. Bay Path systems are to be used in a manner consistent with the policies of the University. Users are prohibited from engaging in any communication that is discriminatory, defamatory and/or unlawful.
6. **Legal Standards**
   All BP Users are expected to abide by all Federal and State laws and regulations. The following list is used for illustrative purposes, and is not intended to be a comprehensive guide to Federal and/or State law:
   - FERPA: regulates the confidentiality of student records.
   - GLBA: regulates the confidentiality of financial information.
   - HIPAA: regulates the security and privacy of health information.
   - PCI DSS: regulates the confidentiality of credit card information.
   - DMCA 1998: regulates the protection of intellectual property.
   - USC Title 18 §1030: Fraud and related activity in connection with computers.
   - CAN-SPAM Act: Regulates the use of mass e-mailing.
   - MGL c.93H: Mandates reporting of security breaches.
   - MGL c.266, S. 33A: Fraud through the use of computer resources.
   - MGL c.266, S. 37E: Prohibits identity theft.
   - MGL c.272, S. 99: Wiretapping law.
   - MA 603 CMR 49: Bullying or Retaliation regulations.
   - MA 201 CMR 16: Regulations on security freezes.
   - MA 201 CMR 17: Standards for the protection of personal information.
   - MA 940 CMR 27: Safeguards for Personal information.
7. **Investigations & Discipline**
   Use of BP systems and data are subject to the Operations Manual for University Employees. Any investigations of misconduct will be conducted according to the Operations Manual. For students, use of BP systems and data are subject to the policies included in the Student Guidebook including the Code of Conduct and Policy on Academic Integrity and Classroom Behavior. Unauthorized use or abuse of BP Systems or data may result in disciplinary action up to and including termination and/or expulsion. Additional civil and/or criminal punishments may be applicable.

8. **Examples of prohibited behavior**
This is not intended to be a comprehensive list of all prohibited behaviors.

- Circumvention of any information security measures, including the hacking, probing, or unauthorized reconfiguration of systems
- Use of computer viruses, worms, or any kind of spyware or malicious software.
- Divulging an account password; unauthorized use of another account or impersonation or misrepresentation of identity
- Removing confidential data from systems or property without adhering to the University's policies regarding data governance
- Storing or transmitting unencrypted, confidential, University data to non-University-owned systems without proper written authorization
- Running unauthorized IT servers or networks
- Using University systems or resources to mine cryptocurrency, including but not limited to Bitcoin or Ethereum
- Forgery of communications, unauthorized or inappropriate manipulation of data (by alteration or omission)
- Sending spam, pranks, chain letters, pyramid schemes, or any kind of for-profit solicitation

- The creation or distribution of data or content that may reasonably be considered disruptive to any member or prospective member of the Bay Path community
- The creation or distribution of data or content that offend someone based on age, gender, gender identity, race, sexual orientation, religious beliefs, national origin, disability, or any other category protected by law
- Illegally downloading, storing, or sharing copyrighted material.
- Engaging in communication that is discriminatory, defamatory, or unlawful.

When you use University computing services, and accept any University issued computing accounts, you agree to comply with this and all other computing related policies.