Last Reviewed: November 2023

Information Security Policy

Purpose and Scope

The purpose of the Information Security Policy (ISP) is to establish security measures to mitigate risk and protect Bentley's IT assets and data from accidental or unauthorized use, disclosure, modification or destruction. Examples of Bentley's information technology (IT) assets and data include critical systems and applications, personally identifiable information, student records, payment card information, and financial assets.

Compliance

Bentley University leadership gives authority to designated IT personnel to establish, implement, and monitor aspects related to the ISP and the Bentley University's Cybersecurity Program ("Program"). Bentley University's Chief Information Security Officer (CISO) maintains authority over and enforcement of the Information Security Policy and related policies. The CIO and the CISO support policy compliance. Compliance with Bentley University's policies and procedures is mandatory, and non-compliance may result in disciplinary action.

Roles and Responsibilities

This section of the document outlines the key information security roles and responsibilities of Bentley leadership teams, faculty, staff and students.

IT/Cybersecurity Subcommittee

The IT/Cybersecurity Subcommittee assists the Board of Trustees in meeting its fiduciary responsibilities with respect to the University's information technology (IT) and cybersecurity programs and risks. The Committee has the authority to review and provide oversight on matters related to the University's IT strategy, risk management, operations, policies and controls.

IT Leadership

The Bentley IT Division has put controls in place to support the ISP and related policies and programs. The Chief Information Officer (CIO) is responsible for overseeing Information Technology (IT), including information security. The Chief Information Security Officer (CISO) has primary oversight and accountability for the Cybersecurity Program. Key IT leadership responsibilities include:

- Designating appropriate personnel to manage and support the Cybersecurity Program and conduct periodic risk assessments of sensitive information and systems.
- Identifying reasonably foreseeable internal and external risks to data/system confidentiality, integrity, availability.
- Adjusting the program to reflect periodic reviews, monitoring, and operational changes.
- Assessing information resources for vulnerabilities and developing and implementing corrective action plans;
- Establishing a process to identify and maintain an inventory of critical assets;

- Classifying information according to its value and sensitivity, and training employees on Bentley's classifications;
- Developing, documenting, and enforcing rules on the acceptable use of information and information assets, and ensuring that faculty and staff are aware of these rules;
- Ensuring that all personnel responsible for securing and maintaining information resources are properly informed about cybersecurity risks and controls;
- Providing leadership in developing clear and effective procedures for response to cybersecurity incidents.

Cybersecurity Office/CISO

The CISO, supported by the IT Division, manages Bentley's Cybersecurity Program. The Program aligns with a national framework – NIST Cyber Security Framework (CSF) – and covers the five functions: Identify, Protect, Detect, Respond, and Recover. Broadly, the CISO and Cybersecurity Team will:

- Work with business partners to identify business/operations changes that may affect cybersecurity practices, policies, and/or standards;
- Understand and communicate specific technology and information security requirements to appropriate groups;
- Lead cybersecurity governance, including committees, policies and procedures;
- Assist with data classifications, risk analyses, audits, and third-party agreements See the Data Classification Policy*;*
- Act as a principal point of contact for cybersecurity-related issues;
- Provide leadership and active participation in cybersecurity incidents;
- Oversee the vulnerability assessment/management program;
- Conduct and/or collect information security risk assessments, and provide guidance;
- Develop cybersecurity training and awareness programs and provide guidance;
- Encourage personnel to raise potential information and cyber security issues with their line managers, the Help Desk, or with the Cybersecurity Team, then track and report information and cybersecurity incidents;
- Participate in access management assessments.

Faculty and Staff

Bentley faculty, staff and students will affirm their responsibilities related to information security by review and acknowledgement of Bentley's Acceptable Use Policy. Disciplinary or corrective action may occur for violations of this policy, or any university policy, in accordance with Bentley's applicable HR policies and procedures.

Policies, Standards, and Procedures

The IT and information security policies are based on risk assessments, business needs, regulatory requirements, changing technologies, emerging threats, and incidents. Bentley University's published policies and procedures can be found on the Bentley.edu website *https://www.bentley.edu/offices/it/policies-all*. Bentley University IT and information security policies will:

- Be available to all faculty, staff and students;
- Support compliance with laws, regulations, contractual obligations, and security requirements;
- Be used by audit and compliance personnel to test controls, and by IT and administrative groups to protect the confidentiality, integrity, availability of Bentley information, systems and assets;
- Be built on a foundation of core information security principles including: authentication, authorization, identification, least privilege, confidentiality, separation of duties, and accountability through appropriate logging and monitoring;
- Be considered for a compliance exception when risk mitigation/acceptance requirements are met. The submitted policy exception form will be reviewed by the CISO.

Cybersecurity Program Components

The CISO will mature the Cybersecurity program by executing on the three pillars of the established framework; Governance, Risk and Compliance, Operations Management and Collaboration, as follows:

I. *Governance Risk & Compliance (GRC)*

i. ***Risk Management Strategy/Framework*** – The IT department and the Cybersecurity team will create processes to identify, analyze, mitigate, and monitor risks to critical information assets. Risks are regularly assessed, prioritized, and managed or remediated in a coordinated manner. Periodic external risk assessments are conducted to document risks and design appropriate controls, and report key risks to senior management in a timely manner. Gaps in secure practices are assessed and remediated;

ii. ***Audits and Risk Assessments*** – The Bentley University IT Division and the Cybersecurity Team will conduct IT security risk assessments and/or will work with consultants and partners for regular audits based on applicable policies, standards, and best practices;

iii. ***Asset / Inventory Management*** – The IT department will maintain an inventory of critical information assets and the owners of those assets;

iv. ***Reporting and Monitoring*** – The Cybersecurity team will establish reporting and metrics to monitor risks and evaluate compliance and the program's effectiveness. They will also utilize evidence-based management and comparative assessments with peer universities;

v. ***Human Resources Security*** – In the event of a violation of this or another IT / information security policy, HR will assess the situation and work with business partners to take the appropriate actions**.**

II. *Operations Management*

i. ***Security Operations*** – The IT department shares responsibility to monitor and protect Bentley systems, prevent a system breach, and avoid data compromise. The department manages a dynamic strategy to keep current with threats, follow best practices, and strive to prevent exposure of university data. Following are the key functions security operation functions:

- **Identify** – The IT/Cybersecurity teams will:
  a. develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities, (for example, asset management);
  b. document, maintain, test and train the designated team members on standard operating procedures;
  c. review system configurations and interoperability to design secure information processing facilities, systems, tools and applications.
- **Protect** – The IT department will:
  a. assign resources to maintain integrity, availability and functionality of critical infrastructure and systems in the event of a breach;
  b. employ measures to minimize the impact of cybersecurity attacks:
  c. manage communications and procedures, as well as alert and/or educate employees of detected threats;
  d. seek to minimize the impact of systems failures that could jeopardize the integrity of software and information;
  e. manage the security of network services, implementing appropriate controls at all critical layers;
  f. maintain the security of information exchanged within the organization and with external entities;
  g. maintain and test business continuity and disaster recovery (BC/DR) plans and strategies.

- **Detect** - The IT department and the Cybersecurity team will:
    a. monitor processes to limit the damage of an attack;
    b. where possible, use layered security and backup systems for coverage to detect suspicious activity;
    c. monitoring the network and systems to detect unauthorized activities and anomalies.

Note: Campus Security and Business Continuity are managed outside of the Cybersecurity Program. Where there are intersections, the CIO and the CISO will work with business partners to formally establish, implement, operate, monitor, review, maintain and improve the Cybersecurity Program.

ii. ***Incident Management*** – The IT department and Cybersecurity team will create and maintain an integrated process for detecting, reporting, responding, recovering, and managing cybersecurity related incidents. The IT department and Cybersecurity teams will follow the *Cybersecurity Incident Response Plan (C-IRP)* and related procedures. The Cybersecurity Incident Response Team (CIRT) will prepare for, detect, analyze, contain, eradicate and/or recover from cybersecurity incidents through the following tasks:

- Execute and maintain response processes and procedures;
- Respond in a timely fashion to detected cybersecurity events;
- Coordinate with internal and external stakeholders as appropriate, which may include external support from law enforcement agencies;
- Conduct activities to prevent escalation of a cybersecurity incident, mitigate its effects, and close the incident;
- Engage in continuous improvement processes by incorporating lessons learned from current and previous events (for example, an after-action review).

iii. ***Access Management*** – Access control methods manage who and what has access to Bentley's systems, applications, and data. The IT division will maintain procedures to manage appropriate access with least privilege to Bentley University's IT systems and protected data. Bentley IT will control access to sensitive data, services and systems using key access controls, including:

- Classification of Bentley information to facilitate appropriate handling based on the Data Classification Policy;
- Granting access only to authorized employees and business partners whose roles require such access;
- Maintaining a process for authorizing, withdrawing and reviewing user access to information systems;
- Putting controls in place to deter theft of information and/or compromise of Bentley systems, applications and processing facilities;
- Requiring Bentley faculty and staff to adhere to policies and standards when using mobile computing, personal devices and/or remote access.

III. *Collaboration*

i. ***Awareness and Training*** – The Cybersecurity team will maintain and improve upon the Bentley-wide Cybersecurity Awareness Program to aid the Bentley community in using best practices to secure data and systems. The CISO will work with partners to establish, effective training on cybersecurity and IT risk management topics. Regular fake phishing campaigns and mandatory cybersecurity training will educate users to deter users from clicking links, attachments, or submitting their credentials. Examples of awareness methods include: email communications, web content, videos, presentations, and cybersecurity awareness events.

ii. ***Vendor Risk Management*** – The IT department and Cybersecurity team uses a risk-based approach for vendor security management. The teams work together to ensure that information systems – *whether on-premise, software as a service (SaaS) or in the cloud* – have appropriate protection controls. Bentley faculty and staff should be aware of and follow requirements outlined in Bentley's Enterprise Applications policy. Vendor risk management requirements include, but are not limited to:

- pre-approval by the CIO, DCIO and/or CISO of any purchase of computer hardware, software, or services, and/or sharing Bentley's data or systems;
- appropriate physical, administrative and technical controls to protect the confidentiality, availability and integrity of Bentley University information and systems;
- annual reviews of Enterprise Application vendor software, systems and security documentation (for example SOC2 Type II reports);
- timely remediation of technical implementations that do not meet security standards.

Related Policies and Procedures

The requirements and responsibilities articulated in this policy are embodied in numerous Bentley policies and procedures, including, but not limited to:

Acceptable Use Policy
Confidentiality Agreement
Data Classification Policy
Records Retention and Destruction Policy
Third Party Policies and Forms
Cybersecurity Incident Response Procedure (C-IRP)
Exceptions Process and Exception Request Form

*Note: A comprehensive list of the policies that function under information security management can be found on the Bentley University website: *https://www.bentley.edu/offices/it/policies-all*.

Contacts and Web Resources

To report a possible information security incident, contact the Help Desk at X3447 or *helpdesk@bentley.edu*. For information security management policy issues or to submit a policy exception, contact Bentley's Cybersecurity Office *cybersecurity@bentley.edu* or the CISO.

Revision History

Version	Date	Author	Reviewers	Approvers	Notes
1.0					Original Document (Written Information Security Program (WISP) and Information Security Policy (ISP))
2.0	4/24/19	Erika PowellBurson, CISO	Vicki Escalera, Director of Compliance and Risk Management; Sue Walsh, DCIO; Dan Sheehan, Director of Client Services; Anne Pugliese, Director of DMAS; Ron Ardizzone, Sr. Manager Technology and Vendor Services	Bob Wittstein, CIO; George Cangiano, VP of HR; Judy Malone, General Counsel	Rewrote existing ISP and added cybersecurity program components. Decommissioned the WISP by adding those elements into the ISP and the Acceptable Use Policy (AUP). The ISP supports Bentley's Cybersecurity Framework and Program.
3.0	11/6/23	David Norman CISO		Liz Hess, CIO	Minor edits and updates to the policy to reflect changes in personnel and procedures