Effective Date: April 24, 2019
Last Reviewed: April 2019
Next Review: April 2020

Acceptable Use Policy

Purpose and Scope

Bentley University's data and information systems are valuable assets which must be protected. Proper and acceptable use of information technology (IT) assets and data will mitigate risks associated with malware attacks, network and system compromises, and data breaches. This Acceptable Use Policy (AUP) applies to the use of Bentley's IT assets, including applications, network, devices, and business systems, whether owned or leased by Bentley, the user, or a third party. All faculty, staff, contractors, consultants, students and guests ("users") of Bentley's devices, networks, and systems must act in a responsible and ethical manner to protect Bentley's systems, information, and reputation. It is expected that all users be familiar with and stay current with this policy.

Definitions

- **Acceptable Use** is the use of information assets (IA) and information technology (IT) resources that is expressly permitted by Bentley University.
- **Breaches** include incidents that result in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms.
- **Disruption** includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- **Information Technology (IT)** encompasses any computing or electronic device related to information assets (e.g. computers, mobile devices, servers, network resources, and IT/security tools).
- **Personally Identifiable information (PII)** is an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such person's: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number that would permit access to an individual's financial account. This does *not* include publicly available information, or government records lawfully made available to the general public.
- **Phishing** is an email-based deception used by criminals to gain access to money, information, and computer systems. Phishing is a type of social engineering. Most phish push you to click a link, open a document, reply back, log into an account, and/or confirm sensitive information.

General Requirements

Bentley University has critical technology and data dependencies for day-to-day operations and strategic goals.

General obligations which you must comply with related to the acceptable use of IT assets include:

1. At all times, users must protect Bentley IT assets and data (regardless of where it is stored or how it is accessed) consistent with the requirements set forth in Bentley University policies and procedures;
2. Users must always protect their credentials (username/password); see password section below for more details;
3. Users must not download Level 1 data to unauthorized locations (e.g. cloud or laptop/desktop) or disclose to unauthorized individuals, systems or entities (e.g. highly confidential, financial, or personally identifiable information). See a supervisor if you have questions. Reference the *Data Classification Policy;*

4. Users are expected to report possible information security incidents to the Help Desk X2854 / *helpdesk@bentley.edu*. Validated incidents will be escalated to *cybersecurity@bentley.edu*;
5. Those who discontinue use of personal devices for work purposes, or who leave Bentley's employ, must have a Bentley IT employee remove business content and disable Bentley-provided software on those devices. These users must also return Bentley-owned devices to their manager or to a Human Resources (HR) representative;
6. **The following activities are strictly prohibited while utilizing Bentley information assets and technology**, **including but not limited to:**
    a. Engaging in any activity that is illegal;
    b. Unauthorized access, duplication, alteration, modification, or destruction of Bentley data, systems, and resources;
    c. Violations of academic integrity and/or the rights of the university or any person. This includes, but is not limited to: selling papers, unauthorized copying of copyrighted material, and installation or distribution of pirated and/or software products that not properly licensed for use by the user and/or Bentley University;
    d. Use of technology resources (e.g. a smart phone) to record conversations, lectures, or classroom interactions without the express consent of those individuals being recorded;
    e. Tampering with or changing anti-virus, firewall, or other security-related computer settings;
    f. Installing prohibited software;
    g. Deliberate introduction of malicious programs onto Bentley systems (e.g., virus; worm; keystroke logger);
    h. Causing or contributing to security breaches or disruptions of network communication. Examples include:
        - Excessive use of systems or network capacity for personal gain/benefit, accessing data without authorization, and logging into a server or account without authorization);
        - Interfering with or denying service to any other user host or Bentley systems;
        - Using a program, script, or command, or sending messages with the intent to interfere with or disable a user's session locally or via the Bentley University network;
    i. Harassment, discrimination, retaliation, or other behavior that violates the university's Code of Ethics and Code of Conduct and other harassment policies. Devices may not be used at any time to harass others based on race, national origin, sex, sexual orientation, gender identity, gender expression, age, disability, religious beliefs, or any other characteristic protected by law;
    j. Making fraudulent offers of products, items, or services originating from any Bentley University account and/or making statements about warranty, express or implied;
    k. Exporting software, technical information, encryption software or technology which may violate International or regional export control laws. (*Consult legal counsel if you have questions on this topic.*)

Note: *The above list is not comprehensive, but rather a means to provide a framework for activities in the category of unacceptable use. Certain users may be exempted from specific restrictions during the course of legitimate job responsibilities (e.g., systems administration staff may be required to disable the network access of a host).*

Passwords and Systems Access

To gain access to Bentley's network, systems and data, authorized users are given credentials (ID and passwords). It is expected that users will follow these password requirements, applicable to individual, system, and application credentials:

1. Users are accountable for all activities associated with their user IDs and passwords (credentials).
2. Users should **never** use their Bentley credentials with non-Bentley applications and/or websites *(e.g. (@bentley.edu email address + network password on a shopping or banking website).*

3. Users must change their passwords upon initial log in and/or when required (e.g. expiration or a password reset by the Help Desk).
4. Users must change their passwords if they suspect a compromise (e.g. shoulder surfing, phishing).
5. Users must keep their passwords secure and confidential. Sharing credentials is prohibited.
6. Users are prohibited from attempting to circumvent authentication and/or security of any computer, host, network, or application account.
7. Passphrases and multi-factor authentication are strongly recommended.

Notice: With the approval of a member of the IT management team, actions may be taken on a Bentley account (e.g. password reset or removal from the network) if there are reasonable indications of a cybersecurity threat.

Phishing and Email Use

All users must be cautious when opening email. A valid-looking email may actually be a phish. A phish is a fake email that looks real. Users should beware of emails that engender feelings of urgency, fear, strong curiosity and exceptional opportunity. Users should report suspicious phishing emails via *phishbowl@bentley.edu* or the report button - see: *https://www.bentley.edu/offices/it/phish-bowl*. ***Note: Bentley will never ask users for their Bentley credentials via phone, text or an email / email link.***

Below are requirements related to emails and phishing which users should follow: See also the *Email Policy*

1. Emails sent or received by users in the course of conducting university business are considered Bentley data, subject to records retention and security requirements. See the *Records Retention Policy*.
2. When conducting university business, users are to use university-provided email accounts, rather than personal email accounts.
3. Incidental/personal use of email should not interfere with Bentley's email system.
4. The following email activities are prohibited when using a university provided email account:
    a. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.
    b. Accessing the content of another user's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the user's official duties on behalf of Bentley University.
    c. Sending or forwarding any email that is suspected by the user to contain computer viruses.

Internet Use

Users accessing the internet through Bentley's network and/or on a Bentley device should do so in a manner that supports business operations and does not interfere with Bentley's business or infringe on the rights of others. The following are examples of inappropriate internet use:

1. Illegal gambling; copyright infringement when file-sharing/swapping; hacking, unauthorized access;
2. Accessing pornographic/adult services sites;
3. Running a sideline internet business without explicit written permission (conflict of interest)

With CIO, DCIO or CISO approval, the IT department may block access to internet websites and protocols that are deemed malicious to the Bentley University environment. The IT Department will periodically review and implement changes to web and protocol filtering rules. If a site is miscategorized, users may request the site be unblocked by submitting a service request to Help Desk X2854 / *helpdesk@bentley.edu*, which will be assigned to a Network/Security Engineer for review.

Remote Access / Personal Devices (BYOD)

Bentley University permits the use of personally-owned devices (e.g. bring-your-own-device / BYOD) to perform work for or on behalf of the university.

Remote Access - IT provides secure remote access technologies (e.g. VPN) for authorized users to access university network and internal resources. VPN is required for privileged accounts and for accessing non-web applications. All remote access to networks owned or managed by the university must be accomplished using a remote access method approved by the university.

When accessing web applications and/or using of personally-owned devices (BYOD), it is expected for users to adhere to these requirements:

1. Non-Bentley devices used to connect with Bentley University data and systems must meet minimum system requirements including, but not limited to:
    a. Password protection
    b. Up-to-date anti-virus protection
    c. Supported web browser and operating systems
    d. Multi-factor authentication where ever possible
    e. Encryption of data in transit and at rest for all Level 1 Highly Confidential data
2. Work data must not be merged with the Bentley users' personal data, nor accessed by unauthorized individuals.
3. Never share Bentley data and applications with unauthorized persons.
4. Users must report lost or stolen devices to Bentley's Help Desk X2854 or *helpdesk@bentley.edu* within 24 hours. Users are responsible for notifying their mobile carrier immediately upon loss of a device.
5. The following are risks, liabilities and disclaimers for using a personal device with Bentley's systems:
    a. University data created and/or stored on non-university devices and databases should be transferred to Bentley resources as soon as feasible;
    b. Bentley reserves the right to disconnect devices or disable services without notification;
    c. The employee is expected to use his or her devices in an ethical manner while on Bentley's network;
    d. The employee is personally liable for all costs associated with his or her device;
    e. When an employee leaves the university, a Bentley IT staff member should assist to delete Bentley data from user's personally owned devices;
    f. The employee assumes liability for personal losses resulting from non-compliance with Bentley policies. This includes, but is not limited to, the partial or complete loss of company and personal data due to an operating system crash, malware, and/or other software or hardware failures.

Social Media

Social media provides users with a means to communicate broadly with the general public. Activities that violate the university's policy against harassment, constitute an invasion of individual privacy, or do not promote free expression undermine the environment that the university seeks to maintain. These actions may result in the imposition of sanctions for violation of university policy. Additionally, untrue statements of fact that harm another's reputation may be defamatory and may subject the individual making such statements to legal action.

Access and Privacy

The university has the legal right to access, preserve and review all information stored on or transmitted through its electronic services, equipment and systems (collectively, "IT Systems"). The university endeavors to afford reasonable privacy for individual users, and does not access information created and/or stored by individual users on its IT Systems except when it determines that it has a legitimate operational need to do so. Signatures from two Bentley vice presidents is required before accessing an employee's email data and/or systems. For the purpose of

performing normal business operations Bentley may share your data with third party providers and/or may operate services in the cloud.

Enforcement

Bentley information technology and assets may be audited and/or monitored for unauthorized activity and usage. Certain kinds of data and IT fraud are illegal and punishable by civil sanctions, criminal fines or imprisonment. The university is obligated to report instances of illegal activities to authorities and will cooperate with authorities in the investigation of illegal activities.

Bentley University reserves the right to require the registration of all technology-related devices used on campus, regardless of whether the device is owned by the institution or an individual. Bentley will identify and quarantine devices suspected of adversely affecting the network; employ tools to monitor network-related activity; and may restrict or eliminate bandwidth allocation to specific devices.

Employee violations will be handled by the employee's supervisor, in conjunction with Human Resources. Student violations will be referred to the Student Affairs judicial process or Bentley's academic integrity process, or both.

Bentley University reserves the right to change provisions of this and other university policies periodically and will provide written notice of substantive changes. Bentley University may take disciplinary action up to and including termination of access, ending of contracts, legal action and/or dismissal of individuals not in compliance with this policy.

Exceptions

Bentley's Chief Information Officer (CIO) maintains authority over and enforcement of the AUP and related policies. Exceptions to this policy may be submitted to the *cybersecurity@bentley.edu* mailbox.

Related Policies and Procedures

The Acceptable Use Policy is one of several university policies and procedures. All university data is classified within security levels, with usage requirements based on data levels. For full details see the university's *Data Classification Policy*. Employees or contractors who process certain types of personally identifiable information, student information, and/or financial information may be bound by the following laws or regulations: 201 CMR 17 – Standard for the Protection of Personal Information of Residents of the Commonweath of Massachusetts; Family Education Rights and Privacy Act (FERPA); Global Data Protection Regulation (GDPR); Financial Services Modernization Act *(GLBA) Policy.* In addition, any individual who handles credit card information on behalf of Bentley University is subject to Bentley's *Payment Card Policy* which supports the Payment Card Industry Data Security Standard (PCI-DSS). The requirements and responsibilities articulated in this policy are embodied in numerous Bentley policies and procedures, including, but not limited to:

Policies:

Code of Ethics (Faculty & Staff)
Code of Conduct (Students)
Data Classification Policy
Digital Millenial Copyright Act
Information Security Policy
Records Retention Policy
(HR) Employment Policies and Practices

Procedures:

Cybersecurity Incident Response Procedure
Policy Exceptions Process and Exception Request Form

Contacts and Web Resources

For immediate reporting of a possible cybersecurity incident, contact the Help Desk at X2854 or *helpdesk@bentley.edu*. For a confirmed cybersecurity incident, an IT risk concern, and/or to submit a request for a policy exception, contact the Cybersecurity Office at *cybersecurity@bentley.edu*.

Revisions

Version	Date	Author	Reviewers	Approvers	Notes
1.0	-	-	-	-	Original document
2.0	4/24/2019	Erika Powell-Burson, CISO	Vicki Escalera, Dir. Compliance & Risk; Sue Walsh, DCIO; Dan Sheehan, Dir. Client Services; Anne Pugliese, Dir. DMAS; Ron Ardizzone, Sr. Mgr. DMAS; Tisha Arffa, InfoSec PM; Judy Malone, General Counsel	Bob Wittstein, VP/CIO; George Cangiano, VP/HR	This updated Acceptable Use Policy (AUP) integrates content from other Bentley policies and thereby replaces the following IT / Security Policies: - The usage portions of the current Data Classification and Usage Policy - Computing and Network Policy - Mobile Device Policy - Clean Desk Initiative - Remote Access Policy Language has been updated based on technology, risk, and regulation changes (e.g. data privacy).
2.1	7/14/2019	Erika Powell-Burson, CISO	Sue Walsh, DCIO; Dan Sheehan, Dir. Client Services; David Norman Judy Malone, General Counsel	Bob Wittstein, VP/CIO; George Cangiano, VP/HR	Added notification that actions may be taken on a Bentley account (e.g. password reset or removal from the network) if there is reasonal indications of a cybersecurity threat.