Effective Date: August 13, 2018

Last Reviewed: October 2024

Next Review: October 2025

CONFIDENTIALITY AGREEMENT

All individuals must read and sign this Confidentiality Agreement prior to beginning their Bentley University work assignment and then annually thereafter. It is the responsibility of each Bentley University workforce member to preserve and protect **confidential information** and systems whether in physical, audio or digital form. Massachusetts laws and regulations (e.g. **201 CMR 17**), Family Educational Rights and Privacy Act (**FERPA**), Gramm-Leach-Bliley Act (**GLBA**), and the Payment Card Industry (**PCI**) establish protections to preserve the confidentiality of personally identifiable information (PII), protected health information (PHI) and cardholder data (CHD). They specify that such information may not be disclosed except as necessary to operations, as authorized by law or by the individual data owner.

Definitions of Confidential Information

- *Personally Identifiable Information (**PII**) is any information that can be used on its own or with other data to identify, contact, or locate a single person. The following data is often used to distinguish individual identity: social security number, full name, email address, home address, passport, etc.*
- *Protected Health Information (**PHI**) is an individual's data in possession of, or derived from, a provider of health care regarding a patient's medical condition, treatment, or history, as well as the patient's and their family members' records, test results, conversations, research records and financial information.*
- *Cardholder Data (**CHD**) is any **PII** associated with a person whose credit or debit card is processed or stored.*
- *Financial information includes: financial activities, billing, and credit and loan information.*
- *University systems, credit and loan information, and business information are also confidential.*

Agreement

In the course of my relationship with Bentley University, I may have access to information that is confidential to Bentley, its students, alumni, donors, employees and/or vendors. In addition to PII, PHI and CHD (defined above), confidential information includes Level 1 Data, financial, employment-related, student record and contractual information related to the University. Any information that is not publicly available is considered confidential.

I will maintain in confidence information that comes to me in the course of my relationship with Bentley and I will not share it with others who do not have a business need to know. When there is a business need to share, I will do so in a manner that limits unauthorized dissemination. I agree to abide by the University's policies on data security, privacy and usage as outlined in the Acceptable Usage Policy.

If I have any questions about the proper sharing of particular information, I will bring the issue to a Bentley manager or supervisor before sharing the information with others. I will contact the HelpDesk (helpdesk@bentley.edu or X2854) for a suspected or actual breach of confidential information.

I agree to follow Bentley's policies and protection requirements (below). I understand that non-compliance may result in disciplinary action up to and including immediate termination of my relationship with Bentley University.

Note that for the purpose of performing normal business operations Bentley may share your data with third party providers and operate services in the cloud.

KEY PROTECTION REQUIREMENTS

1. It is my legal and ethical responsibility to protect the privacy, confidentiality, integrity and availability of all Bentley University information and systems that I use and come in contact with. I understand that unauthorized access, use or disclosure of such data and systems is strictly prohibited.

2. All of Bentley's Information Technology (IT) resources (including but not limited to: computers, mobile devices, copiers, email, internet access, systems, and applications) are the property of Bentley University and should be used for business purposes. Incidental personal use of IT resources is permissible so long as the activity is not illegal, does not conflict with workplace needs or policy, and does not result in added cost and/or a security breach to the University. Usage of Bentley's data and systems is monitored and periodically audited for compliance with policies.

3. Access, use, or dissemination of confidential information is only permitted when required by job role in accordance with this Confidentiality Agreement. Deliberate unauthorized access or release of confidential information may subject me to disciplinary action up to an including immediate termination and/or legal action.

4. When I access confidential information, I will only use the minimum necessary information and access required to do that function of my job. I will not alter or change existing information unless I am certain of its accuracy and I am authorized to make the change.

5. I will use secure means to perform my job duties. I am prohibited from downloading confidential information to portable media and/or uploading to the cloud unless I am authorized to do so and I use acceptable encryption.

6. I will secure my access credentials (log-in user ID & password) and I will not share them with anyone. I will not re-use my Bentley ID and password to access non-Bentley systems - e.g. email; social networking sites; online shopping sites.

7. Upon separation, I will promptly return all Bentley resources, including but not limited to data and devices.

8. I understand that email containing confidential information must be sent securely. Emailing from my Bentley.edu email to another Bentley.edu email address is secure. For emails sent outside of Bentley I will ensure they are sent securely and any sensitive data is adequately protected.

9. I will contact the HelpDesk (helpdesk@bentley.edu or X2854) with information regarding actual or suspected loss, theft, improper use of, or access to confidential information and systems - e.g. attempts to collect login credentials (phishing) or suspicious attachments (malware).

10. I will read and follow the policies found on the Bentley University website including but not limited to the University's Information Security Policy, and additional IT and security policies.

Signature: ____

Printed Name: ____

Title: ____

Department: ____

Dated: ____