BENTLEY UNIVERSITY

Data Classification Policy

Purpose and Scope

Bentley University's data and information systems are critical to Bentley University operations and must be protected based on risk and legal requirements. This Data Classification Policy defines risk classification levels and minimum protection requirements. Complying with these requirements will protect Bentley's data from unauthorized access, modification, disclosure, transmission, destruction, or breach of applicable laws and regulations. Business and data owners must protect university data regardless of the environment, sponsor, and/or media.

Compliance

Bentley University's Chief Information Officer (CIO) maintains authority over and enforcement of the Data Classification Policy and related policies. The Deputy CIO and the Chief Information Security Officer support policy compliance. Bentley University reserves the right to change this and other university policies periodically and will provide written notice of substantive changes.

Exceptions to this policy should be submitted to the *cybersecurity@bentley.edu* mailbox.

Data Classification Definitions and Levels

All university data are classified based on risk

Data classification, in the context of information security, is the classification of data based on sensitivity levels and the impact to the university should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine appropriate baseline security controls for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications, as follows:

Level 1 – Highly Confidential: Data are classified as Level 1 / Highly Confidential when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates (e.g. data breach, identity theft, fraud, systems failure, loss of business opportunities or competitive advantage, etc.). Data protected by law or contract, or data deemed by Bentley University leadership as highly sensitive are examples of Level 1 data. Level 1 data require the greatest level of data privacy and security controls.

Level 2 – Bentley Confidential: Data should be classified as Level 2 / Bentley Confidential when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. Level 2 data require that a reasonable level of security controls be in place. By default, all university data that is not explicitly classified as Level 1 or Level 3 data should be treated as Level 2 data.

Level 3 – Public: Data classified as Level 3 / Public have no expectation of privacy or confidentiality. There is minimal or no risk if data are exposed, compromised, altered or destroyed. This data may be disclosed to any individual or entity inside or outside of the university.

Examples of Data Types

Data Classification Type	Types of Data	Application Examples

Level 1 / Highly Confidential
 	
High Risk and Strong Security Controls
	• Personally Identifiable Information (PII) including first and last name in conjunction with any of the following:
	  ○ PINs; passwords; biometric data
	  ○ Social Security Number (SSN); Passport number
	  ○ Driver's license number; state-issued ID card number
	  ○ Financial account numbers; access codes
	  ○ Payment card; Cardholder Data (CHD)
	• Data source / backups
	• Systems / Security Data – e.g. passwords; database; cryptography keys; unredacted network or systems diagrams; vulnerabilities, etc.
	• Protected Health Information (PHI)
	  ○ Patient billing; medical records; family health/history
	  ○ Information about physical or psychological state of health
	  ○ Disease, medical history/treatment, drugs, genetic test results
	• Student data, including judicial/disciplinary information; Student's permanent record, Transcripts, and/or grade reports
	• Alumni data including last name, first name with any of the following:
	  ○ Telephone/fax numbers, email, and employment information
	  ○ Family information (spouse, partner, guardian, children, grandchildren)
	  ○ Donation amount and assets
	• Strategic data
	• Board of Trustees (BoT) records
	  ○ Meeting Minutes
	  ○ Board of Trustees votes
	  ○ Confidential information communicated at BoT meetings and/or shared with board members
	• Research data containing personally identifiable information from internal and external sources
		Enterprise Resource Planning (ERP tool)
		
		Campus Police Safety
		
		Health Services
		
		Counseling
		
		Financial Aid
		
		Security tools
		
		Data warehouse
		
		Document image management system
		
		Study abroad
		
		Research data containing personally identifiable confidential information

Level 2 / Bentley Confidential
 	
Moderate Risk and Reasonable Controls
	• Bentley private or proprietary research:
	  ○ Anonymous data collected by researchers through interviews, surveys and other methods
	  ○ Research data protected through vendor agreements
	• Business intelligence
	• File share servers and/or storage
	• Employee (Faculty and Staff) and Student Records, eg.:
	  ○ Bentley University number; visa numbers
	  ○ Personnel records, salary data, performance reviews, benefits
	  ○ Date of birth, place of birth, mother's maiden name
	  ○ Promotion and tenure files (e.g. tenure decision notes)
	  ○ Race, ethnicity, nationality, and/or gender
	  ○ Background information including:
	  ▪ Credit/criminal background checks; convictions
	  ▪ Private directory/contact information
		Course Evaluation
		
		Student Record Management
		
		Facilities
		
		Institutional Research
		
		Identity Management
		
		Research Data: HCUP and anonymized health data

Level 3 / Public Low Risk and No Expectation of Privacy or Security	• Public directory information (unless otherwise restricted) • Any content or image on the university's public web sites • Publicly released press statements • University course catalog • Job postings • Campus map • Public research sources	Marketing materials Press Releases Bentley.edu web pages Bentley Social Media Bureau of Labor Statistics Tables US Census Surveys

Policy Requirements

The highest level of security controls must be applied to Level 1 / Highly Confidential data, and a reasonable level of security controls for Level 2 data. Level 3 / Public data has no explicit privacy or security requirements. Data in either electronic or physical (e.g. paper) format shall be destroyed in accordance with the University's Record Retention and Destruction Policy.

The required minimum data protection standards are listed below:

Minimum Data Protection Standards

Minimum Protection Requirements	Level 1 Highly Confidential	Level 2 Bentley Confidential	Level 3 Public
1. Use of this data must not violate university policy or any applicable laws and regulations	required	required	required
2. Only authorized users may access or change the data	required	required	required
3. Login credentials (user name/password) are required, unique, and kept confidential	required	required	required
4. Two-factor authentication	required	recommended	not required
5. Encrypt credentials and data during transmission via secure authentication methods	required	required	not required
6. Encrypt data at rest	required	strongly recommended	not required
7. Only store data on authorized devices*, and in approved and secured locations	required	strongly recommended	not required
8. Data sharing with vendors and third-parties requires a vetted contract and a security review	required	required	not required
9. Store printed materials securely	required	required	not required
10. Destroy data according to university policies and procedures	required	required	not required
11. Make data available to the public	prohibited	prohibited	acceptable

**Authorized devices include Bentley OneDrive, Bentley Sharepoint or Teams sites, Bentley provided laptops, Bentley's Azure environment*

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
Information Security Policy
Records Retention and Destruction Policy
Vendor Risk Management Documents
Policy Exceptions Process / Exception Request Form
Enterprise Applications Policy

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

Contacts and Web Resources

For immediate reporting of a possible information security incident, contact the Helpdesk at X3447 or *helpdesk@bentley.edu*

For information security questions, or to request a policy exception, contact *cybersecurity@bentley.edu*

Revision History

Version	Date	Author	Approvers	Notes
1.0	1/29/2010	IT/Security	Information Privacy Committee	Original Document
2.0	9/30/2013	IT/Security	Information Privacy Committee	Rev 2
3.0	2/28/2019	Erika Powell-Burson, CISO Tisha Arffa, InfoSecurity PM	CIO	- Tightened L1 / L2 / L3 definitions - Renamed L1 to “Highly Confidential; L2 to “Bentley Confidential”; L3 to “Public” - Updated minimum data security standards and examples, adding 3 new controls (#’s 4, 6, 8) - Moved handling controls to the Acceptable Use Policy - Moved record retention and data destruction controls to the Record Retention and Destruction Policy - Updated contact information
3.1	1/29/2020	Mike Gioia, ISO	DCIO	Updated Minimum Protection Requirements – Removed #8 Risk assessments and #12 social media
3.2	5/13/2021	Mike Gioia, ISO	Data Privacy Committee	Annual Review. No changes
3.3	4/4/2023	David Norman, CISO	CIO	Updates to include research data and list of authorized devices
3.4	11/10/2023	David Norman CISO	CIO	Minor updates to links