BENTLEY UNIVERSITY

IT / Information Security Policy Exception Request

Policy Exception Request Form

Bentley University policies were created based on business, legal, and regulatory requirements which Bentley is obligated to meet. If you'd like to apply for an exception to an IT or Information Security policy, then complete this request form and email it to cybersecurity@bentley.edu with the subject line "POLICY EXCEPTION." Please follow the instructions as listed below:

Step 1 - Complete the fields below, then email to cybersecurity@bentley.edu

I. Exception Request / Risk Description:

1. **Exception Requestor, Including Divisional Manager**

2. **Description of the Policy Exception Being Requested Including Relevant Policy Excerpts**

3. **Description of Risk Involved**

4. **Explanation for Why an Exception is Requested**

5. **Business Justification for the Exception Request**

6. **Data Involved, Including Classification – L1, L2 or Public and/or System** (see Data Classification Policy)

7. **Duration of the Exception Request - Start and end date**

II. Approval

1. **Mitigating Controls -** The Cybersecurity Team (CISO or delegate) will work with the exception requestor and key users to detail the mitigating controls to reduce risk to the university.
**Note whether the mitigating controls are short-term or on-going. Include any relevant information such as: hardware, software, infrastructure, training and procedural documentation, administrative and support personnel, consultants, disaster recovery, back-up, business continuity, monitoring, etc.*

2. **Approved Exception Dates**

3. **Expiration**

Step 2 – Email cybersecurity@bentley.edu, using "POLICY EXCEPTION" as the subject line, and CC your manager. Attach your completed Policy Exception Request Form to the email along with any additional supporting documentation. The Chief Information Security Officer (**CISO**) will consider the exception request for approval / denial. The requestor (and based on risk, the division manager) should review and comment regarding concerns, support, and/or if further information is needed.

Step 3 – CISO Validates Risk and Determines Status – Once the Cybersecurity Team (CISO/ delegate) receives the email, s/he will validate the initial risk (High/Medium/Low) assigned – making adjustments if/as needed. Based on the results of the risk assessment, one of the following statuses will be assigned:

a. **APPROVED –** The Exception Request is approved and forwarded (if/as needed) to the appropriate group for changes.
b. **PENDING -** Request is pending; other options or modifications may be suggested for consideration.
c. **DENIED -** Request denied. The Head of Compliance will provide supporting feedback.
d. **N/A -** Not applicable; no exception is necessary.
e. **EXPIRED –** The exception has reached the duration of the approved request and must be reassessed to continue.

Step 4 – CISO Communicates status. The CISO or delegate will communicate the exception status and applicable dates.

***Confidential information** includes PII; PHI; and CHD (see definitions below); University systems, financial activities, billing, credit and loan information, business information. Personally identifiable information (**PII**) includes social security number, name, email, home address, phone number, etc. and may extend to other data when paired with the prior, and student records. Protected Health Information (**PHI**) is an individual's data in possession 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.*