Bentley University Endpoint Protection Policy

1. Purpose

This policy establishes requirements for protecting university owned and personal endpoints (such as desktops, laptops, and mobile devices) at Bentley University. By implementing robust endpoint protection measures, we aim to safeguard sensitive data, prevent unauthorized access, and mitigate risks associated with endpoint vulnerabilities.

2. Scope

This policy applies to all Bentley staff, faculty, contractors, and third-party vendors who utilize endpoints to access organizational resources and sensitive data, regardless of ownership (university-owned or personally owned).

3. Definitions

- **Endpoint**: Any device (hardware or virtual) that interacts with Bentley University's networks or data.
- **Bentley Owned Device:** Any endpoint device (laptop, desktop, or mobile device) owned and provisioned by Bentley IT.
- **Personally Owned Device:** Any endpoint device (laptop, desktop, or mobile device) not owned or provisioned by Bentley IT.
- **Sensitive Data**: Information that requires special protection due to its confidential, proprietary, or regulatory nature. This is defined in Bentley's Data Classification Policy as level 1 or level 2 data.
- **Privileged Access:** The administrative level of access to a system that permits management of user roles or permissions, impersonation, or other restricted system configuration activities.
- **Administrative Credentials:** Bentley accounts created for the sole purpose of providing privileged access to Bentley provisioned systems or services.

4. Access to Sensitive Data

4.1. Level 1 university data should not be stored on any endpoint devices. See Bentley's Acceptable Use Policy and Data Classification Policy for details.
4.2. See Bentley's Acceptable Use Policy for details about securing data access on personally owned devices.
4.3. Full time staff or faculty privileged access to Bentley systems should only be allowed on Bentley owned devices using administrative credentials.
4.4. Privileged access to Bentley systems by contractors or non full-time employees should be managed through vendor agreements or other controls approved by Bentley Cybersecurity.

5. Registration and Compliance

5.1. All Bentley owned endpoints must be listed in Bentley's asset inventory.
5.2. Compliance with this policy is mandatory for all endpoints connected to the Bentley network that are either university or personally owned.

6. Minimum Protection Requirements for Bentley Owned Endpoint Devices

6.1. Access to the endpoint is password protected and conforms to the Bentley University password protection requirements. Authentication credentials should never be shared.
6.2. The endpoint is running vendor-supported operating systems that are automatically updated, with up-to-date security patches installed in a timely manner. Patches to mitigate critical vulnerabilities are installed as soon as possible.
6.3. Anti-virus, anti-spyware and monitoring programs are installed to perform continuous and scheduled scanning to detect and/or prohibit unauthorized access. The virus definition list is updated at least once daily.
6.4. Installed utilities for staff and faculty devices such as BIOS are configured for access, where possible, with unique passwords.
6.5. The endpoint is configured to automatically lock after no more than 15 minutes of inactivity.
6.6. The endpoint configuration conforms to the university security policy of "least privilege" and administrative access to Bentey University owned endpoints is restricted and audited.
6.7. Endpoints and mobile devices used to access Bentley data should use full-disk encryption.

6.8. Bentley owned endpoint devices are physically protected and access is not shared with other individuals.

7. Recommended Protection Requirements for Personal Devices

The recommendations outlined below represent the minimum protections for managing or processing Bentley data on personally owned devices:

7.1. The device login is protected by a password, pin code, or biometrics (for example, fingerprint, face, or other scan).
7.2. The device encrypts all stored University data.
7.3. The device is configured to lock automatically after a period of inactivity.
7.4. If mobile, the device has a mechanism for a secure remote wipe if it is lost or stolen.
7.5. If mobile, the device contains a recovery mechanism using a GPS tracking system.

8. Enforcement

Bentley Information Technology reserves the right to audit and monitor **all** endpoint devices connected to the Bentley network. Bentley also reserves the right to register all technology related devices, including endpoints, on campus regardless of whether the device is owned by the institution or the individual. Bentley also reserves the right to quarantine devices suspected of deviating from this policy, or devices that may adversely affect the security of the university environment.

9. Exceptions

Bentley's Chief Security Information Officer (CISO) maintains authority over, and enforcement of, this policy. Requests for exceptions to this policy may be submitted to cybersecurity@bentley.edu.

4. Related Policies and Procedures

This 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.

5. Revisions

Version	Date	Author	Reviewers	Notes
1.0	4/18/2024	David Norman		Original Document
1.1	4/29/2024	David Norman	Dan Sheehan, Lisa Duhaime	Team feedback and updates
1.2	6/6/2024	David Norman	Dan Sheehan, Lisa Duhaime	Additional feedback and comments on document draft
1.3	7/1/2024	David Norman	IT SMT	Additional input from IT SMT