2022 Policy Changes Highlighted in Yellow

Summary of Policy

Bechtel has an obligation to protect information, including the information of our employees, our customers, and other business partners, from the unauthorized or improper access or disclosure. This Access and Use Policy (AUP) assists Bechtel in complying with this obligation. Anyone who wants to obtain or maintain the right to use Bechtel Computing Resources and Bechtel Information must comply with this AUP.

Bechtel uses various tools to monitor Bechtel devices and infrastructure to protect and secure information. All data and information created, transmitted, stored, or received on Bechtel devices or Bechtel's network and systems is subject to monitoring. Bechtel will use and disclose such data and information consistent with applicable law and this AUP.

With respect to any information passing through or stored on Bechtel Computing Resources, Users must understand that, while Bechtel will abide by the applicable data protection and data privacy laws in relation to Personal Information, (a) Users do not have rights or expectations of privacy except as provided by those laws; (b) such Personal Information may be monitored, intercepted, and searched by Bechtel or an authorized third party on its behalf; and (c) such Personal Information, including any information that an employee has stored on Bechtel-provided devices or other Bechtel Computing Resources and not deleted upon termination, may be disclosed or used by Bechtel in each case as described in this Policy.

Users must:

- Use Bechtel Computing Resources for Bechtel business purposes
- Protect and not share user IDs, passwords, and authentication tokens
- Not alter, disable, or modify information security controls
- Handle information in accordance with Bechtel's policies and otherwise a manner consistent with Bechtel's business interests
- Only use approved software and cloud services for conducting business
- Honor all copyright requirements
- Apply the highest ethical standards when accessing web sites or using Bechtel email consistent with the Bechtel Code of Conduct
- Report any theft, damage, or loss of Bechtel Computing Resources or Bechtel Information
- Ensure security protections are in place on all computing resources connecting to a Bechtel network
- Cooperate fully with any investigation regarding an allegation of behavior that involves compliance with this AUP
- Understand and expect that Bechtel can and does monitor activities on Bechtel Computing Resources.
- Exercise best practices when opening or reading email
- Follow Bechtel policies and procedures when using personal devices to access Bechtel networks or information resources.

PURPOSE

This document discusses your role in assisting Bechtel in securing Bechtel Computing Resources and Bechtel Information. It discusses the terms of access and use enabling: 1) the protection of Bechtel Computing Resources and Bechtel Information; 2) an understanding of internet and email restrictions; 3) what to do if assets are stolen, damaged, or lost; 4) an understanding of mobile and personal devices and their use; 5) restrictions on removable media; and 6) how Bechtel monitors activity to understand and protect assets. Bechtel is serious about securing Bechtel Computing Resources, Bechtel Information.

SCOPE

The terms of this AUP must be complied with by anyone who wants to obtain or maintain the right to access and use Bechtel Computing Resources and Bechtel Information. This AUP applies both to Bechtel employees and others who are permitted access to and use of Bechtel Computing Resources and Bechtel Information.

ACCESS AND USE

General

Bechtel Computing Resources are intended to be used for Bechtel business purposes. Incidental personal use by Users is permitted, provided such use is kept to a minimum, does not interfere with Bechtel business, and is not contrary to Bechtel's business interests. With respect to any information passing through or stored on Bechtel Computing Resources, Users must understand that, while Bechtel will abide by the applicable data protection and data privacy laws in relation to Personal Information, (a) Users do not have rights or expectations of privacy except as provided by those laws; (b) such Personal Information may be monitored, intercepted, and searched, by Bechtel or an authorized third party on its behalf consistent with those laws; and (c) such Personal Information, including any information that an employee has stored on Bechtel-provided devices or other Bechtel Computing Resources and not deleted upon termination, may be disclosed or used by Bechtel, in each case as described in this AUP.

Bechtel requires the use of password protections on Bechtel Computing Resources and any Personal Device connected to Bechtel Computing Resources. Users should never share their passwords or tokens with anyone, including Bechtel IS&T staff.

Any activity intended to disable, damage, or circumvent information security controls put in place by Bechtel is prohibited. Such prohibited activities include, but are not limited to, attempting to crack passwords; attempting to decode encryption; introducing malicious software; installing tools designed to monitor, hide, or erase activity; modifying Bechtel-issued security tools used to access Bechtel Computing Resources; uninstalling Bechtel-installed anti-virus software; improperly using another User's password; or using a system left logged on by another User.

Susceptibility to Phishing Attacks

Bechtel conducts regular phishing exercises to assist with User behavior relating to this attack vector. Failure of these exercises is managed in a fashion to lessen User susceptibility to phishing attacks. Bechtel has adopted a progressive approach that includes training, counseling, potential termination of account access, and potential termination of employment.

Handling Bechtel Information

Bechtel either owns or is responsible to other parties for Bechtel Information maintained on Bechtel Computing Resources. Some Bechtel Information is considered sensitive, either to Bechtel or to another party, and some Bechtel Information is subject to protection under various laws. Users must handle Bechtel Information in a manner consistent with the business interests of Bechtel and in compliance with all applicable confidentiality obligations, use restrictions and applicable laws.

Users must not transmit or otherwise disclose outside of Bechtel any Bechtel Information that has been labeled or classified as "confidential", "strictly confidential" or the like without authorization in writing. In addition, personally identifying information, sensitive or protected medical information about an individual, and Bechtel Information that is proprietary to a company other than Bechtel, as well as information proprietary to Bechtel should be protected with encryption.

When using cloud services, special caution should be exercised to ensure all Bechtel business is conducted using only cloud services vetted and approved Bechtel or the Customer. If you have questions on what cloud services are authorized, contact your local IS&T for assistance.

Internet Use and Copyright Infringement

Users must not access websites related to sex, pornography, gambling, hate speech, criminal activities, or illegal drugs, or use email for such purposes. Users must not download, store, or transmit any inappropriate or offensive electronic material, such as material that contains or references any type of fraudulent, illegal, harassing, offensive, or obscene activity.

Bechtel is committed to honoring the copyrights of software, media, and other information owners and complying with their licensing requirements and/or copying restrictions. Users must not download, install, use, or copy software or media that is not licensed and approved for use by Bechtel. Users must comply with all restrictions applicable to software or media installed or stored on Bechtel Computing Resources. Bechtel's Legal Department can provide guidance as to the copyright constraints applicable to particular information, and Bechtel IS&T can provide guidance as to license restrictions applicable to particular software acquired or managed by Bechtel.

Theft, Damage, or Loss

Users are responsible for safeguarding Bechtel Computing Resources issued to them. Theft, damage, or loss of any Bechtel Computing Resources or Bechtel Information, or of any Personal Device containing Bechtel Information, must be reported immediately to Bechtel IS&T, which may report the loss to Bechtel Security and/or local authorities as appropriate. Bechtel will not be responsible for the theft, damage, or loss of any Personal Device. Theft, damage, or loss of any Bechtel Business Partner computing resources must be reported immediately to the Business Partner.

Use of a Personal Device

Personal Devices pose a significant information security risk when used to access Bechtel Computing Resources. Use of a Personal Device for such access is a privilege, not a right, and is subject to special considerations and requirements to protect Bechtel's legal and security interests. **Any User who does not agree with and follow these requirements must not use a Personal Device to access Bechtel Computing Resources.**

Any tablet, smart phone, laptop, or desktop Personal Device used to access Bechtel Computing Resources or store Bechtel Information must have the following installed and enabled:

(a) password required for access to the Personal Device;
(b) lockout when the Personal Device has been inactive (e.g., for more than 15 minutes); and
(c) up-to-date security and operational patches for the Personal Device's operating system.

In addition, any laptop or desktop Personal Device used to access Bechtel Computing Resources or store Bechtel Information must have current anti-virus protection software installed and configured so that all files are scanned for viruses or other forms of malicious software before they can be saved to disk or opened for viewing.

Bechtel Information may not be stored on a Personal Device unless necessary to perform a job function, and then only to the limited extent necessary. Upon the termination of a User's right to access Bechtel Computing Resources

(e.g., termination of employment or termination of account access), the User must delete all Bechtel Information on all Personal Devices.

By using a Personal Device to access Bechtel Computing Resources or store Bechtel Information, or otherwise agreeing to abide by this AUP, a User agrees that Bechtel may physically and electronically access the Personal Device and the data on it, as described below, in the event of:

(a) a security incident potentially involving the device;
(b) an alleged breach of the terms of this AUP;
(c) a subpoena or other legal requirement relating to Bechtel Information stored on the device; or
(d) a preservation hold request to the User instituted by Bechtel's Legal Department.

In any such event Bechtel may require the User of a Personal Device to provide Bechtel IS&T with physical or electronic access to the device, in unlocked mode, for as long as reasonably necessary to comply with legal requirements or to complete the applicable investigation. Users shall not delete information or change any settings, software, or configuration after Bechtel requests access to the Personal Device. Users are required to comply and cooperate with any request for such access that may be made by Bechtel. To the extent permitted by applicable law, Bechtel will have no liability to a User in connection with lawful access to a Personal Device or to Personal Information stored on a Personal Device in any such event.

Users should be aware that Bechtel may have the technical ability to delete remotely all information stored on a Personal Device. A remote "wiping" of the device by Bechtel could result in deletion of Personal Information as well as Bechtel Information. It is Bechtel's AUP only to use this capability in a situation where either:

(a) the device has been lost or stolen,
(b) there has been a suspected security compromise of the device, or
(c) the User's right to access Bechtel Computing Resources has been terminated and Bechtel cannot ascertain in a timely manner that Bechtel Information stored on the device has been deleted.

Bechtel will make reasonable efforts to consult with the User before taking action to wipe a User's Personal Device. Any action by Bechtel to wipe a Personal Device without the consent of the User will be subject to applicable law. To the extent permitted by applicable law, Bechtel will not be responsible for the loss of a User's Personal Information if Bechtel determines that a wiping action is necessary to protect the security of Bechtel Computing Resources and/or Bechtel Information.

General Mobile Device Usage Guideline

Bechtel strives to provide technology that supports the business and mission needs of Bechtel and its Business Partners, but this requires the User to understand and utilize best practices, including the following:

(a) Modifications to the Bechtel issued SIM Card is not permitted.
(b) The User of the personal Mobile Device is not permitted to make any modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system, also known as "jailbreak"). If the device is detected as 'jailbroken', it will no longer be permitted to access Bechtel Computing resources and it may be remotely wiped.
(c) Encryption is required for all Bechtel provided laptops, hard drives, and other portable devices.

Mobile Applications

Bechtel recognizes that it may be necessary or customary in certain jurisdictions to use applications on Mobile Devices to conduct Bechtel business. It is incumbent upon each individual User to make sure any Bechtel Information and related communications transmitted, received or conveyed on Mobile Devices are retained consistent with Bechtel's document retention policies and the Bechtel Code of Conduct.

While not encouraged, Bechtel does not forbid the installation or use of messaging applications/services on Bechtel issued or Personal devices (e.g. WhatsApp, Signal, Telegram, etc.). The decision to use these

applications/services is a personal and voluntary one based on privacy and other concerns as well as the market conditions the User works in. However, if messaging applications/services are used, each individual User is responsible for ensuring that (a) no sensitive or confidential Bechtel business Information is transmitted or sent via these applications/services and (b) any Bechtel Information and/or related communications received from or sent to third parties (e.g., customers/contractors/partners) are managed and retained consistent with Bechtel's document retention policies and Bechtel's Code of Conduct.

The preferred Bechtel messaging service that can be used with Bechtel information is Microsoft Teams. Teams can be installed on both Bechtel and Personal Mobile Devices and used with your Bechtel account.

Use of a Removable Storage Device

Removable storage devices, such as USB drives, constitute a heightened information security risk and therefore, are restricted from use at Bechtel unless there is a valid business requirement which has been reviewed and approved. Users must not connect personal removable storage devices to Bechtel Computing Resources or use such devices to store Bechtel Information. To the extent that there is an approved business exception to use a removable storage device, then only a Bechtel or Bechtel Business Partner provided device should be used and subject to the following terms:

(a) Bechtel Information should be copied from Bechtel Computing Resources to a removable storage device only as a temporary transfer mechanism.
(b) A User must never make a copy of data on a removable storage device and then delete the original data stored on Bechtel Computing Resources.
(c) Bechtel Information that is characterized or labled as "confidential", "strictly confidential" or the like must be encrypted. (Bechtel IS&T can provide technical guidance on encryption.)
(d) A removable storage device containing Bechtel Information must be locked up or otherwise securely stored when not in use.
(e) Bechtel Information stored on a removable storage device must be deleted from the device after the business need for such storage has been fulfilled.

Maintain a Secure Workspace

At all locations:

- Always handle Bechtel Information according to its information classification.
- When not actively in use, keep confidential information out of view and stored in locked rooms, containers, drawers, cabinets, etc.
- When leaving the workspace, screen lock or electronically lock (Ctrl-Alt-Del) all computing and mobile devices.
- Conduct audio communications in a secure manner. Verbal communications and recorded sessions shall only be audible by authorized parties. Speaker phones shall only be used in physically controlled locations. Do not leave a device connected to a phone call or conference call unattended.
- Remove the documents from printers, photocopiers and/or scanners immediately on completion.
- Hard copies no longer required must be disposed of securely (shredding machine or shredding bin).
- Any portable storage device containing Bechtel Information must be secured per the instructions published in the Removable Media Device Usage Policy.

At physically unsecured locations, in addition to the above,

- Always protect Bechtel Information, whether from being seen or heard by unauthorized personnel.
- When not actively in use, keep all non-public business information out of view and stored in locked rooms, containers, drawers, cabinets, etc.

- When unattended, computing or communication devices containing, handling, or managing Bechtel information must be physically secured (e.g., cable lock, taken with you, etc).

Use of the Computing Resources of a Bechtel Business Partner

All of the terms of this AUP apply to the personnel of a Bechtel Business Partner accessing or using Bechtel Computing Resources. Bechtel may require a Bechtel Business Partner to execute separate access/use agreements as a condition of access to Bechtel Computing Resources and to better protect Bechtel Information.

Where a User desires to access Bechtel Computing Resources using the computing resources of a Bechtel Business Partner, Bechtel IS&T will work directly with the Business Partner to provide such access in a manner that is designed to protect the information security interests of both Bechtel and the Business Partner. Bechtel Information may not be stored on Business Partner computing resources unless necessary to perform a job function, and then only to the limited extent necessary.

MONITORING AND ENFORCEMENT

Bechtel reserves the right in its sole discretion to deny the privilege of access to and use of Bechtel Computing Resources and/or Bechtel Information to any User who demonstrates that they cannot or will not comply with the terms of this AUP.

Bechtel may access information stored on or passing through Bechtel Computing Resources and may inspect and monitor any Bechtel Computing Resources, when appropriate, for the following purposes (the **Monitoring Purposes**):

- as necessary to pursue Bechtel's legitimate interests in:
    - conducting its ordinary business activities (limited to appropriate access to resources as necessary because of User's absence or their having left Bechtel);
    - ensuring and enforcing compliance with Bechtel's information security and other policies;
    - protecting Bechtel Computing Resources and Bechtel Information;
    - analyzing usage and other information with a view to:
        - identifying and implementing opportunities to improve Bechtel Computing Resources and other aspects of Bechtel's business processes; and
        - predicting Users' behavior in their use of Bechtel Computing Resources and their work with Bechtel generally, so as to anticipate and address potential problems and opportunities;
    - conducting, and (where relevant) co-operating in relation to law enforcement and similar agencies in relation to, investigations into apparent or suspected disciplinary, legal and/or regulatory issues;
    - collecting and disclosing information relevant to legal and other disputes; and
- as necessary to comply with Bechtel's legal and contractual obligations.

Users must understand that Bechtel, in exercising its access, inspection, and monitoring rights for the Monitoring Purposes, may access information that a User may consider private or sensitive if it is stored on or passes through Bechtel Computing Resources. This may involve access both to the content of communications and other documents created using or submitted to Bechtel Computing Resources and to information recorded by Bechtel Computing Resources including metadata about their use (for example, the date and time of an email and the address to which it was sent; or information as to sites accessed on the Internet; or information as to internal resources accessed). Access to Personal Information for the Monitoring Purposes, as described above, is mandatory and not based on Users' consent.

Any Personal Device, Mobile Device, or removable storage device used to access Bechtel Computing Resources will be subject to remote monitoring and inspection by Bechtel IS&T for the Monitoring Purposes. As a User, by using a Personal Device to access Bechtel Computing Resources or store Bechtel Information or otherwise agreeing to abide by this AUP, you (a) acknowledge that, while Bechtel will abide by the applicable data protection and data privacy laws in relation to any Personal Information stored on such devices, you have no right or expectation of privacy with respect to that device except as provided by those laws, and (b) will make the device available for inspection upon request. Bechtel Business Partner computing resources will not be subject to inspection by Bechtel without the express consent of the Business Partner.

Consequences of a User's violation of the terms of this AUP may include the temporary or permanent loss of the privilege of access to and use of some or all Bechtel Computing Resources and/or Bechtel Information. For Bechtel employees, violation of this AUP may also result in disciplinary action, up to and including termination of employment.

Suspected abuses of Bechtel Computing Resources or of Business Partner computing resources or other suspected violations of the terms of this AUP should be reported to abuse@bechtel.com, as well as to the appropriate Bechtel management contact and the appropriate Bechtel Business Partner contact (if applicable).

DISCLOSURE AND INTERNATIONAL TRANSFER

In accordance with applicable law, Bechtel may disclose Personal Information collected for the Monitoring Purposes as described above to:

- law enforcement and similar agencies, as necessary to comply with Bechtel's legal obligations and otherwise cooperate with them (this may include voluntary disclosure);
- persons or parties to whom Bechtel is obliged to disclose, or to whom it is in Bechtel's interests to disclose, Personal Information in the context of litigation and other disputes;
- other Bechtel companies;
- service providers who process Personal information on Bechtel's behalf; and
- other persons to whom Bechtel is required by law to disclose Personal Information.

These disclosures may involve transfers of Personal Information to the USA and other countries outside the European Economic Area, including countries which do not have data protection laws which are as protective of Personal Information as the data protection laws within the European Economic Area. Where Bechtel transfers Personal Information to other members of the Bechtel group of companies (other than in the USA), or to service providers, in these countries, Bechtel will ensure that the information is protected by data transfer agreements in a form approved for this purpose by the European Commission. Personal Information transferred to members of the Bechtel group of companies in the USA is protected by the commitments that the Bechtel group of companies makes through its participation in the EU-US Privacy Shield Framework.

RETENTION AND DELETION OF PERSONAL INFORMATION

Personal Information collected for the Monitoring Purposes as described in this AUP will be deleted when it is no longer needed, given the purposes for which it is held, in accordance with Bechtel's records management policies and the specific records retention schedule for the project or activity for which the record was created. Users may contact the Bechtel Privacy Officer at privacy@bechtel.com for more information on record retention periods.

USERS' RIGHTS UNDER EUROPEAN DATA PROTECTION LAW

Users granted access to Bechtel Computing Resources and/or Bechtel Information by Bechtel offices or other establishments within the European Economic Area have various rights under applicable European data protection

law in relation to Bechtel's processing of their Personal Information collected for Monitoring Purposes. In particular, they can:

- request access to their Personal Information and various other information about its processing;
- request that their Personal Information is corrected or deleted if it is inaccurate; and
- object to the processing of their Personal Information, or (in some circumstances) require the processing of their Personal Information to be 'restricted' (so that the information is not deleted, but its active use is suspended).

DEFINITIONS

For purposes of this AUP:

Bechtel means the Bechtel group of companies, or any one of the Bechtel companies, as the context may require.

Bechtel Business Partner means a customer, joint venture partner, supplier, or other company with whom Bechtel has an agreement relating to access and use of Bechtel Computing Resources and/or Bechtel Information, and/or access and use of the Business Partner's computing resources or information. Such access may be by inter-company network connection or via the Internet.

Bechtel Computing Resources include Bechtel's global Project Services Network and all Internet connections, desktop and laptop computers, servers, systems, networked devices, hard drives, memory devices, and removable storage devices owned, controlled, and/or managed by Bechtel. However, for purposes of this AUP, Bechtel Computing Resources do not include temporary Internet connections provided as a courtesy to guests in a Bechtel facility.

Bechtel Information for purposes of this AUP means software or data that is located on or that passes through Bechtel Computing Resources. Bechtel Information also includes information that is proprietary to Bechtel or a Bechtel Business Partner and information in Bechtel's custody that personally identifies individuals.

Information Owner is the original source or author of the information. If information originates outside Bechtel, such as a client, the Information Owner is the initial Bechtel recipient of the information. The Information Owner of Bechtel Information can be a particular individual, or the leader of a department, project, or other work group (e.g., for a department or discipline database) (ref. RIM-MI 120, *Information Security Classification and Protection Responsibilities*).

Information Custodian means individuals who have been given access to Bechtel information are referred to as Information Custodians. (ref. RIM-MI 120, *Information Security Classification and Protection Responsibilities*).

IS&T means Bechtel's Information Systems and Technology group, which manages Bechtel Computing Resources.

Mobile Device is a small computing device that allows connectivity to Bechtel Computing Resources or Bechtel Information using wireless technology.

Personal Device means a device that is not owned, controlled, or managed by Bechtel or a Bechtel Business Partner. A Personal Device can be a public computer, a home desktop computer, a laptop, a tablet computer (e.g., Apple iPad), a smart phone (e.g., Apple iPhone or Android), or a removable storage device (e.g., USB drive, DVD, or backup hard drive).

Personal Information means software or data that is purely personal to, or otherwise relates to, a User.

User means any individual who accesses or uses Bechtel Computing Resources and/or Bechtel Information.

CONTACTING BECHTEL

Questions to Bechtel IS&T may be directed to the IS&T Service Center, at ISTSC@bechtel.com, or the User's local Bechtel IS&T support staff.

Additional information about Bechtel's policies relating to access and use of Bechtel Computing Resources and Bechtel Information is available through the IS&T Service Center.

If Users have questions about Bechtel's privacy practices or wish to exercise the data protection rights described above or to be provided with copies of the data transfer agreements also described above , they should contact the Bechtel Privacy Officer privacy@bechtel.com.

Users granted access to Bechtel Computing Resources and/or Bechtel Information by Bechtel offices or other establishments within the European Economic Area are also entitled to lodge complaints about Bechtel's processing of their Personal Information with European data protection authorities, in the country in which they work or in which the relevant Bechtel establishment is located (at their option).

ACKNOWLEDGEMENT

I acknowledge that I have read and understood and will abide by the requirements of this Access and Use Policy.