

INFORMATION TECHNOLOGY
ACCEPTABLE USE STANDARD
2026

BRG
Berkeley Research Group

Contents

CONTENTS **2**

I. PURPOSE AND SCOPE **3**

1.1 PURPOSE 3
1.2 SCOPE 3
1.2.1 Applicability of Assets *3*
1.2.2 Applicability to Staff and Temporary Workers *3*
1.2.3 Applicability to External Parties *3*
1.3 REFERENCES AND RELATED DOCUMENTS 4

II. AGREEMENT **4**

2.1 CONFIDENTIAL INFORMATION 4
2.2 GENERAL INFORMATION SYSTEMS SECURITY 7
2.3 EQUIPMENT USE 8
2.4 UNACCEPTABLE USE 10

IV. DOCUMENT MAINTENANCE **12**

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

I. Purpose and Scope

1.1 PURPOSE

BRG's information systems enable the firm's professionals to respond to clients' needs more quickly and efficiently. However, with these systems come risks that require appropriate security and usage guidelines. While these technology resources are excellent business tools, we must use all systems wisely.

1.2 SCOPE

The Information Technology (IT) Acceptable Use Standard (AUS) is intended to promote the usage by firm's professionals of all forms of IT assets while providing guidelines designed to protect the interests of our clients and the firm.

1.2.1 Applicability of Assets

The scope of this standard includes all electronic assets that are owned or leased by BRG. Assets may include but are not limited to:

- Computers (laptops, desktops, virtual, etc.)
- Servers
- Network and Internet infrastructure
- Mobile computing devices
- Electronic media
- Non-electronic media

1.2.2 Applicability to Staff and Temporary Workers

This Standard applies to all individuals employed by BRG, including full and part-time employees, affiliates and contractors ("BRG personnel").

1.2.3 Applicability to External Parties

This Standard applies to all external parties, including but not limited to BRG business partners, vendors, suppliers, outsource service providers, consultants, affiliates and other third party entities with access to BRG networks and system resources.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

1.3 REFERENCES AND RELATED DOCUMENTS

- Information Security Policy
- Data Classification and Protection Standard

II. Agreement

2.1 CONFIDENTIAL INFORMATION

This section outlines BRG's policies and procedures for handling Confidential Information, which is defined as referenced in the BRG Data Classification Standard:

1. All sensitive client information including, but not limited to, financial records, case materials, bank account numbers, Social Security numbers, and Protected Health Information ("PHI") as defined by the Health Insurance Portability and Accountability Act ("HIPAA").
2. All confidential BRG information including, but not limited to, business records, financial information, contracts, and employee personal information.

BRG policies and procedures are designed to protect Confidential Information from unauthorized access or use, loss or theft, and to ensure that BRG is in full compliance with generally accepted business practices as well as laws and requirements, such as HIPAA.

All BRG personnel shall adhere to the following guidelines with respect to Confidential Information.

1. *Notification Requirement:* If you suspect that any Confidential Information has been improperly disclosed, lost or stolen, or that the security of Confidential Information has otherwise somehow been compromised, you must contact the IT Department **immediately**. Similarly, if you suspect that the security of any BRG IT system has been compromised, whether Confidential Information was involved or not, you must immediately contact the IT Department and advise them of the circumstances. The IT Department will log the information and notify the Legal Department.

2. *Handling of Confidential Information:* BRG enforces strict policies regarding the use of computer systems and provides training to all personnel employed by BRG on the use and handling of Confidential Information. BRG personnel should be aware of the following policies.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

a. Confidential Information shall only be stored on BRG-approved equipment.

b. Unless approved by the client (with respect to client Confidential Information) or in writing by BRG's General Counsel (with respect to BRG Confidential Information), Confidential Information should not be stored on non-encrypted devices including, but not limited to Home Computers, CDs, DVDs, Flash (Thumb) Drives, Blackberry, Android, iPhone, iPads, or other outside, non-BRG media or devices.

c. All BRG approved mobile devices used to send, receive, or store Confidential Information, including emails, contacts and appointments, shall be encrypted and protected with passwords.

d. Access to client files shall be restricted to employees working on the project. Changes to access rights for case files require approval from an authorized person (i.e., anyone already with authorized access to the case file or any member of the Legal Department) When requesting access to a case file include the authorization you have received for such access.

e. All BRG laptop and desktop computers shall be encrypted.

f. BRG has installed software on all desktop and laptop computers to prevent writing any information to non-encrypted USB Flash (Thumb) Drives. The software does not prevent writing information to other forms of non-encrypted removable media, such as CDs and DVDs, though transferring Confidential Information to such media is prohibited by this Policy. The IT Department has posted instructions for encrypting data when using removable media, which can be found on the BRG Intranet.

g. Unless authorized by the Case Manager or Expert and the Legal Department in writing, Confidential Information protected by HIPAA shall not be transferred over standard email as attachments or in the body of a message. When sending or receiving Confidential Information protected by HIPAA, BRG's Encrypted File Transfer Protocol portal (using Accellion kiteworks software) or similar client provided encrypted method should be used. Contact the IT Department if you need assistance with the Accellion kiteworks software.

h. All BRG users who store Personal Health Information (PHI) as part of their work responsibilities are required to store such information exclusively within BRG's HITRUST-certified environment. The use of any other storage location or platform for PHI is strictly prohibited. This policy is intended to ensure compliance with applicable regulations, maintain the security and confidentiality of PHI, and uphold BRG's commitment to data protection and privacy.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

Our clients' information is confidential and has been provided to us in the context of a trusted consulting relationship. When you use, reference, or store that information please be cognizant of both the clients' expectations and the parameters outlined in this Policy.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

2.2 GENERAL INFORMATION SYSTEMS SECURITY

This section of the policy defines the rules and requirements related to the secure and reliable operation of BRG's information systems infrastructure ("the BRG network).

1. All network user accounts require complex passwords. Passwords must be at least 15 characters long and contain a combination of at least two capital letters, numbers, or symbols. Passwords should not be related to a user's job or personal life (e.g., a car license plate, spouse's name, dates or address). Passwords must not be written down or stored in any location, electronic or otherwise, where unauthorized persons might discover them.

2. All BRG approved mobile devices require a 4-digit password (i.e., letters and/or number characters).

3. BRG has installed firewalls, anti-virus, anti-spyware, network monitoring, intrusion detection systems, and other technology to mitigate malicious attacks on the BRG network. Users shall not disable any of these systems.

4. Connecting any equipment to the BRG network is strictly prohibited without consent from the IT Department. This includes, but is not limited to, computers, removable media (thumb drives), cameras, mobile devices, and printers.

5. No software, including, but not limited to, iTunes, screen savers, and toolbars, should be installed on any BRG equipment without prior authorization from the IT department, unless there is an immediate and legitimate business need. If any software is installed the IT Department should be notified as soon as possible.

6. All personnel employed by BRG have a duty to report computer security incidents, violations and problems to the IT Department on a timely basis so that prompt remedial action may be taken. It is not the job of non-technical workers to assess the severity or the urgency of these incidents, violations, and problems.

7. Use network drives to save files whenever possible. BRG does not backup laptops or desktops and will not be able to recover any deleted or corrupted files that are saved locally. If you require offline access to these files, please contact the IT Department to enable 'Offline Folders.'

8. In addition to the BRG network, BRG provides a guest network with access to the Internet only. BRG personnel may provide non-BRG personnel with the password to access to the guest network only.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

9. The use of a personal Virtual Private Network (VPN) on BRG's corporate network is prohibited as it can compromise BRG's implemented security controls.

2.3 EQUIPMENT USE

As a person employed by BRG, you may be issued computer equipment and/or given access to systems and software as part of the tools needed to conduct business. Your specific responsibilities related to BRG systems and equipment are outlined in this section of the policy.

All phone equipment, computer equipment and software provided to you by BRG (BRG systems) are the exclusive property of BRG. The use of this equipment is intended for firm-related business purposes. Reasonable, incidental personal use of the BRG systems is appropriate and permissible; however, BRG systems and equipment should not be used as a substitute for your own personal computing needs. **Misuse or abuse of this Policy may result in denial of some or all personal use privileges or disciplinary action, up to and including termination.**

BRG respects the individual privacy of its employees. However, employee privacy does not extend to work-related conduct or to the use of BRG's provided equipment, systems, or supplies. Email is a written form of communication. Employees who utilize any email program on BRG computers, regardless of whether provided by BRG, should understand that such messages are not private. Email programs have been provided and allowed on BRG systems to facilitate business communications. Although each employee has an individual password to access BRG's email, the system belongs to the Firm and the contents of email communications must be and are accessible at all times to BRG's management for any business purpose. Therefore, do not assume that any message you send or receive on BRG equipment, even if personal in nature, is confidential and not subject to BRG review. Backup copies of email may be maintained and referenced for business and legal reasons. Any use of the email system constitutes consent to the disclosure of transmissions to authorized BRG personnel. Since your personal email messages can be accessed by BRG management without prior notice, you should not use email to transmit any message you would not want read by a third party. You should never use these systems for such purposes as soliciting for commercial ventures, religious or personal causes, outside organizations, or other similar, non-work related solicitations. If the Firm discovers that you are misusing any of its email systems, or any other BRG computer system, you will be subject to disciplinary action, up to and including termination.

You may not use BRG's email system in any way that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale. Forbidden transmissions include: sexually explicit messages, cartoons, jokes, unwelcome propositions, love letters, ethnic or racial slurs, or any other messages that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, disability, age, national origin, or religious or political beliefs. Use of BRG's email system in violation of these guidelines will result in disciplinary action, up to and including termination.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

Incidental access to online personal email systems such as Yahoo, Gmail and Hotmail is not prohibited. However, accessing email from a web browser bypasses many of the Company's security systems. Please be extremely careful when opening attachments or clicking on links. Do not open any executable attachments, scripts, or other programs without checking with the IT Department first. Be cautious when opening any emails that you are not expecting, even from people you know. If you are not sure whether an email or its attachment is safe, please contact the IT Department.

It is important to remember that technology cannot replace common sense. Be extremely careful opening emails requesting any account information or offering money.

Be cautious when clicking on links while browsing the Internet. Avoid clicking on the contents of popup windows. Developers of viruses and spyware often create web pages that mimic anti-virus software or offer to speed up your computer. If you suspect a virus or any other type of intrusion or infection is affecting your BRG computer or the BRG network, please contact the IT Department immediately.

Watching streaming video, playing online games or downloading of large graphic files is prohibited unless there is a legitimate business need. These transmissions can have a significant adverse impact on our network performance and interfere with the ability of other users to work efficiently.

BRG tries to provide all of the software necessary for an employee to conduct their job responsibilities and maintains a number of licenses for various software programs. Please contact the IT Department request any new software or licenses and before purchasing any software. If software must be accessed or purchased immediately and no one from the IT Department is available, please notify the IT Department of the purchase as soon as reasonably possible.

Any unauthorized duplication of licensed software is prohibited by BRG and in violation of the Federal Copyright Laws. No software licensed by BRG shall be installed on any equipment without prior approval of the IT Department. If the IT Department is unavailable and there is an immediate need to install the software, you must notify the IT Department as soon as reasonably possible.

Only BRG IT Department staff is allowed to make modifications to computer equipment or software. In the event that maintenance or repair is required, you must contact the BRG IT Department to arrange for such maintenance or repair. You shall not attempt to make any repairs without express permission from a member of the BRG IT Department. You agree to comply with all federal, state, and local laws while using BRG computer equipment.

BRG expects that you will take reasonable care in preserving BRG's equipment in excellent condition while it is in your possession, including, but not limited to the adhering to the following guidelines:

1. Do not check computer equipment as luggage when traveling. It must be carried on.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

2. Do not leave computer equipment in a car. If you must do so, leave the equipment in the trunk of the car or where it is not visible.
3. Do not leave computer equipment in the open, unlocked, or in an unprotected area.

4. Do not leave your computer or mobile device unattended in public areas, such as restaurants and bars.

5. If any equipment is lost, stolen, or damaged you must notify the IT Department as soon as reasonably possible.

You will surrender and return any BRG equipment or property immediately upon written or oral request from BRG. In addition, you will surrender any computer equipment and software should you breach this Policy, or upon the termination of your employment or other business relationship with BRG. All emails residing on personal equipment, including mobile devices, shall be deleted upon termination. You are required to send an email or letter confirming you have completed this requirement.

The policies set forth above are subject to change and you will be advised of these changes as they occur.

2.4 UNACCEPTABLE USE

The following activities are examples of unacceptable use of BRG electronic communications:

- Engaging in any activity that is illegal under Local, State, Federal or International law in conjunction with the usage of BRG's electronic communications systems.

- Unauthorized transmission or collection of Confidential or Personally Identifiable Information (PII). Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations.

- Unauthorized reproduction of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which BRG or the user does not have a specific and active license.

- Exporting software, technical information, or technology in violation of International or regional export control laws.

- Introduction of malicious programs into the State's electronic communications systems infrastructure including, but not limited to, computer workstations, servers, and networks.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

- Circumventing user authentication or security of any account, host, or network, including disclosing a user's password to others or allowing a user's account to be used by others.
- Interfering with or denying electronic communications system services to any user.

- Inappropriate purposes, in violation of the intended use of the network, as defined by this standard. Interference or disruption of network users, services, or computers, including distribution of unsolicited advertising, and/or propagation of computer viruses.

- Effecting security breaches or disruptions of any electronic communications system. This includes, but is not limited to tampering with the security of BRG's computers, network equipment, services or files.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

IV. Document Maintenance

Ownership of the Document:	Chief Information Security Officer
Date Created:	November 24, 2014
Date Last Revised:	December 12, 2025

Reviewer / Approver

Name	Title	Role	Date
Chip Goodman	Principal Information Officer	Information Security Officer	December 24, 2014
Chip Goodman	Principal Information Officer	Information Security Officer	April 15, 2015
Chip Goodman	Vice President of Information Technology	Information Security Officer	December 24, 2015
Chip Goodman	Vice President of Information Technology	Information Security Officer	December 24, 2016
Chip Goodman	Vice President of Information Technology	Information Security Officer	August 31, 2017
Chip Goodman	Vice President of Information Technology	Information Security Officer	September 20, 2018
Chip Goodman	Vice President of Information Technology	Information Security Officer	December 9, 2019
Chip Goodman	Vice President of Information Technology	Information Security Officer	December 8, 2020
Chip Goodman	Vice President of Information Technology	Information Security Officer	January 18, 2022
Chip Goodman	Vice President of Information Technology	Information Security Officer	December 8, 2022
Chip Goodman	Vice President of Information Technology	Information Security Officer	December 7, 2023
Chip Goodman	Vice President of Information Technology	Information Security Officer	December 9, 2024

Change History

Rev.	Date	Change Author	Modification
Version 1	December 24, 2014	Chip Goodman	Template change.
Version 2	April 15, 2015	Chip Goodman	Template modification.
Version 3	December 24, 2015	Chip Goodman	Annual review.
Version 4	December 24, 2016	Chip Goodman	Minor edits and annual review.
Version 5	August, 31, 2017	Chip Goodman	Review and signature.
Version 6	September 20, 2018	Chip Goodman	Annual review.
Version 7	November 11, 2019	Scott Mohorek	Annual review.
Version 8	November 02, 2020	Scott Mohorek	Annual review.
Version 9	January 14, 2022	Thomas Sudar	Minor edits and annual review.
Version 10	November 07, 2022	Thomas Sudar	Annual review.
Version 11	November 17, 2023	Thomas Sudar	Annual review.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.

Version 12	November 17, 2024	Thomas Sudar	Annual review.
Version 13	November 26, 2025	Thomas Sudar	Annual review, inclusion of PHI environment requirement, inclusion of personal VPN being prohibited, new owner.

This document is the property of Berkeley Research Group. It contains information that is proprietary, confidential, sensitive or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to Berkeley Research Group. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Berkeley Research Group executive management.