BRG

INTELLIGENCE THAT WORKS



Information Security Policy

Revised July 2026

Table of Contents

1 Purpose and Overview

2 Scope and Definitions

2.1 Scope

2.2 Confidential Information Defined

3 Confidential Information Requirements

3.1 Notification Requirements

3.2 Handling of Confidential Information

4 General Information Systems Security

4.1 Network and Password Security

4.2 Systems Monitoring and Incident Reporting

4.3 Guest Network and Content Sharing

5 Equipment Use

5.1 Ownership and Permitted Use

5.2 Email and Communications Systems

5.3 Internet Use and Security Precautions

5.4 Software and Licensing

5.5 Equipment Care and Return

1. Purpose and Overview

Berkeley Research Group, LLC (together, collectively, with its subsidiaries and affiliates, "BRG" or the "Company") is committed to protecting the confidentiality, integrity, and availability of its information and the information entrusted to it by clients. This Information Security Policy ("Policy") establishes BRG's procedural requirements and technical guidelines for the protection of confidential information and the provision of secure, reliable systems.

This Policy applies to all individuals employed by BRG, including full- and part-time employees, affiliates, and contractors ("BRG personnel"). Please read this document carefully and contact the IT Department or Legal Department with any questions. A full listing of policies relating to BRG's Information Security Program is available on the BRG Intranet.

2. Scope and Definitions

This section identifies who is covered by the Policy and defines the key concepts of information that BRG treats as confidential and subject to heightened protection.

2.1 Scope

This Policy applies to all BRG personnel, affiliates, independent contractors, and subcontractors worldwide (collectively, "BRG personnel"). BRG's policies, standards, and procedures are designed to protect Confidential Information from unauthorized access or use, loss, or theft, and to ensure that BRG remains in full compliance with generally accepted business practices as well as applicable laws and requirements, such as the Health Insurance Portability and Accountability Act (HIPAA).

2.2 Confidential Information Defined

"Confidential Information" includes, but is not limited to, the following categories:

- All sensitive client information, including financial records, case materials, bank account numbers, Social Security numbers, and Protected Health Information (PHI) as defined by HIPAA.
- All confidential BRG information, including business records, financial information, contracts, and employee personal information.

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

3. Confidential Information Requirements

This chapter sets forth BRG's requirements for reporting suspected compromises of Confidential Information and for the day-to-day handling of Confidential Information by BRG personnel.

3.1 Notification Requirements

If you suspect that any Confidential Information has been improperly disclosed, lost, or stolen, or that the security of Confidential Information has otherwise 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 or not Confidential Information was involved, you must immediately contact the IT Department and advise it of the circumstances. The IT Department will log the incident and notify the Legal Department.

3.2 Handling of Confidential Information

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

- Confidential Information shall only be stored on BRG-approved equipment.
- Unless approved by the client (for client Confidential Information) or in writing by BRG's General Counsel (for BRG Confidential Information), Confidential Information should not be stored on non-encrypted devices, including home computers, CDs, DVDs, flash (thumb) drives, smartphones, tablets, or other outside, non-BRG media or devices.
- All BRG-approved mobile devices (laptops, smartphones, tablets, etc.) used to send, receive, or store Confidential Information, including emails, contacts, and appointments, shall be encrypted and protected with passwords.
- Access to engagement files shall be restricted to personnel 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.
- All BRG computers shall be encrypted.
- BRG has installed software on all desktop and laptop computers to prevent writing information to non-encrypted USB flash (thumb) drives. This software does not prevent writing information to other non-encrypted removable media, such as CDs and DVDs, though transferring Confidential Information to such media is prohibited by this Policy. Instructions for encrypting data on removable media are posted on the BRG Intranet.
- Unless authorized by the Engagement 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. Use BRG's Secure File Transfer Protocol (SFTP) portal (Accellion kiteworks) or a similar client-provided encrypted method instead. Contact the IT Department for assistance with Accellion kiteworks.

4. General Information Systems Security

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

4.1 Network and Password Security

- 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 relate to a user's job or personal life (e.g., a car license plate, spouse's name, dates, or address) and must not be written down or stored anywhere unauthorized persons might discover them.
- All BRG-approved smartphones and tablets require a 4-digit password (letters and/or numeric characters).
- 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.
- Connecting any equipment to the BRG network is strictly prohibited without consent from the IT Department, including computers, removable media, cameras, smartphones, tablets, and printers.
- No software, including unlicensed software, screen savers, and toolbars, should be installed on any BRG equipment without prior IT Department authorization, unless there is an immediate and legitimate business need. If software is installed, the IT Department should be notified as soon as possible.

4.2 Systems Monitoring and Incident Reporting

- All BRG personnel 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 responsibility of non-technical personnel to assess the severity or urgency of these incidents.
- Use BRG systems designed for sharing content (Teams, SharePoint, OneDrive, file shares, databases, etc.) to save files whenever possible. If offline (off-network) access to shared resources is required, contact the IT Department for assistance.

4.3 Guest Network and Content Sharing

In addition to BRG's Corporate network, BRG provides a BRG Guest network with access to the Internet only. BRG personnel may provide non-BRG personnel with the password to the Guest network only.

5. Equipment Use

As a person employed by BRG, you may be issued computer equipment or given access to systems and software as part of the tools needed to conduct business. This section outlines your responsibilities related to BRG systems and equipment.

5.1 Ownership and Permitted Use

All phone equipment, computer equipment, and software provided to you by BRG ("BRG systems") are the exclusive property of BRG. Use of this equipment is intended for firm-related business purposes. Reasonable, incidental personal use 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.

5.2 Email and Communications Systems

BRG respects the individual privacy of its employees; however, employee privacy does not extend to work-related conduct or to the use of BRG-provided equipment, systems, or supplies. Email is a written form of communication, and messages sent or received on BRG systems are not private. Although each employee has an individual ID and password, the email system belongs to the Firm, and the contents of email communications must be, and are, accessible at all times to BRG management for any business purpose. Backup copies of email may be maintained and referenced for business and legal reasons. Any use of the email system constitutes consent to disclosure of transmissions to authorized BRG personnel.

You may not use BRG's email system in any way that may be seen as insulting, disruptive, or offensive, 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 could be construed as harassment or disparagement based on sex, race, sexual orientation, disability, age, national origin, or religious or political beliefs. Violations will result in disciplinary action, up to and including termination.

Incidental access to online personal email systems (e.g., Yahoo, Gmail, etc.) is not prohibited; however, accessing email through a web browser may bypass BRG's security systems. Be extremely careful when opening attachments or clicking on links, and do not open executable attachments, scripts, or other programs without first checking with the IT Department.

5.3 Internet Use and Security Precautions

Technology cannot replace common sense. Be extremely careful opening emails that request account information or offer money, and be cautious when clicking links or pop-up windows while browsing the Internet, as developers of viruses and spyware often mimic anti-virus software or offers to speed up your computer. If you suspect a virus or other intrusion is affecting your BRG computer or the BRG network, contact the IT Department immediately.

Watching streaming video, playing online games, or downloading large graphic files is prohibited unless there is a legitimate business need, as these activities can adversely impact network performance and interfere with other users' ability to work efficiently.

5.4 Software and Licensing

Contact the IT Department to request new software or licenses, and before purchasing any software. If software must be accessed or purchased immediately and no one from IT is available, notify the IT Department of the purchase as soon as reasonably possible. Any unauthorized duplication of licensed software is prohibited by BRG and violates Federal Copyright Laws; no software licensed by BRG shall be installed on any equipment without prior IT Department approval. Only BRG's IT Department staff may make modifications to computer equipment or software — contact IT to arrange any needed maintenance or repair.

5.5 Equipment Care and Return

BRG expects that you will take reasonable care in preserving BRG's equipment while it is in your possession, consistent with the following guidelines:

Traveling with Equipment

Do not check computer equipment as luggage when traveling — it must be carried on.

Equipment in Vehicles

Do not leave computer equipment in a car. If you must do so, leave it in the trunk or where it is not visible.

Unattended Equipment

Do not leave computer equipment in the open, unlocked, or in an unprotected area, including your computer, smartphone, or tablet in public places such as restaurants and bars.

Lost, Stolen, or Damaged Equipment

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, and you are required to send an email or letter confirming that you have completed this requirement.

The policies set forth in this document are subject to change, and you will be advised of any changes as they occur.