

Information Security Policy

At Level7, one of our top priorities is making sure that all information belonging to us, our clients and our staff is protected and kept secure at all times to protect the privacy, interests and intellectual property of all parties involved. All Level7 personnel, including employees and contractors, are required to comply with the following requirements at all times while using Level7's software, workstations or other equipment or resources; or while working with any code, documents, digital assets, data or any other form of information belonging to Level7 or its clients:

Workstation Security

1. Security requirements described in this section apply to in-office workstations as well as workstations used for remote work, regardless whether the device is owned by Level7 or belongs to the employee/contractor.
2. All workstations must require a password to access the system and the data stored therein.
3. All workstations must be kept in a locked state (that requires a password to resume the work) when not in use.
4. All workstations must run the latest version of the operating system and be updated on a regular basis.
5. If an employee/contractor's workstation is used both for the personal and professional use, all data related to Level7 and its clients must be kept separate from any other data.
6. Computers located in publicly accessible area (eg. library, university etc.) CANNOT be used as a workstation.
7. In case the workstation is used by more than one user (whether the other user(s) work for Level7 or not), all data related to Level7 and its clients must be stored in a way that is accessible only to Level7's employee/contractor.
8. All work for Level7 must be done using either Chrome, Brave or Firefox browser in their latest version. Use of any other browser must be first approved by Level7.
9. Web browsers used for Level7 work cannot have any extensions installed other than ones that are necessary to perform the work or have been approved by Level7. If an employee/contractor uses their personal device for work, they can create a separate user profile in their browser to help satisfy this requirement.
10. Installation or use of any non-work related or unauthorized applications on Level7-owned workstations is prohibited.
11. If an employee/contractor is authorized to use their personal device for Level7 work, they are responsible to ensure that all applications installed on that device are trusted & secure and do not present any threat to Level7 data stored on, or accessed with that device.
12. All workstations must use a modern, well known and highly rated antivirus, anti malware or similar security software. Workstations running Linux are exempt from this requirement.
13. No employee/contractor should perform any work for Level7 or access data belonging to Level7 or any of its clients, while outside of the United States, unless they have been authorized to do so in writing.
14. If an employee/contractor is authorized to use their personal device for Level7 work, they are required to create and maintain regular backups of all Level7-related and locally stored data. Such backups are subject to the same security controls as the original data they are a copy of.

Phone

(877) 7-LEVEL7 (877-753-8357)
(720) 600-6202

Email & Website

L7.io
info@L7.io

Corporate Address

1942 Broadway St, STE 314C
Boulder, CO 80302

Network security

1. All work must be done while using a secure, dedicated connection. Use of a publicly available network (eg. WIFI network in the airport, hotel, university, coffee shop or other public area) is not permitted unless VPN is used to secure the connection.
2. Use of unprotected WIFI networks (not requiring password to connect) is prohibited.
3. Transfer of any data belonging to Level7 or its clients over an unencrypted network (eg. HTTP without SSL or unencrypted FTP) is prohibited.
4. Connections to Level7 networks, network devices, servers and other remote resources should be closed while not in active use. This includes any SSH, RDP, FTP/SFTP connections, as well as mounted network drives and devices (such as SSHFS, SMB or FUSE).

Data security

1. All sensitive, critical or classified information must be stored on a medium that provides encryption at rest (eg. encrypted hard drive/partition, encrypted cloud storage etc.)
2. Level7 employees/contractors are allowed to maintain active access only to data necessary for them to perform their current assignments. If the employee/contractor gets reassigned to a different department or task, or gets removed from a project, they are no longer authorized to access data no longer needed to advance their current work.
3. When the employee/contractor's employment agreement or contract with Level7 ends, they are required to surrender all Level7's data in their possession and delete it from their personal workstation (if applicable) afterwards.
4. Level7 employees/contractors are required to comply with, and enforce all data-retention policies that are applicable to data under their control.



Password Security

1. Only secure passwords can be used. Secure password is a password meeting the following criteria:
 - a. Contains a combination of letters (upper- and lowercase), numbers and special characters
 - b. Is of a sufficient length (at least 10 characters)
 - c. Does not contain any dictionary words or ordered sequences of numbers or characters (eg. "12345", "abcde") or sequences of several repeated characters (eg. "1111", "aaaa" etc.)
 - d. Does not contain significant portions of any non-protected information about the account its meant to protect, ie. username, account number etc.
2. All passwords must be unique. Same password cannot be used in more than one device, application or resource.
3. All passwords must be stored in a password manager that utilizes end-to-end encryption. If an employee/contractor was given access to Level7's password manager, all passwords related to Level7's clients, data or applications must be stored in that password manager.
4. Individually assigned passwords should never be shared with anyone, including other Level7 contractors/employees, with the exception of the company owner and IT admin.
5. When the employee/contractor's employment agreement or contract with Level7 ends, they are required to surrender all personally created work-related credentials to the Level7's IT admin or other designated personnel.

Phone

(877) 7-LEVEL7 (877-753-8357)
(720) 600-6202

Email & Website

 L7.io
 info@L7.io

Corporate Address

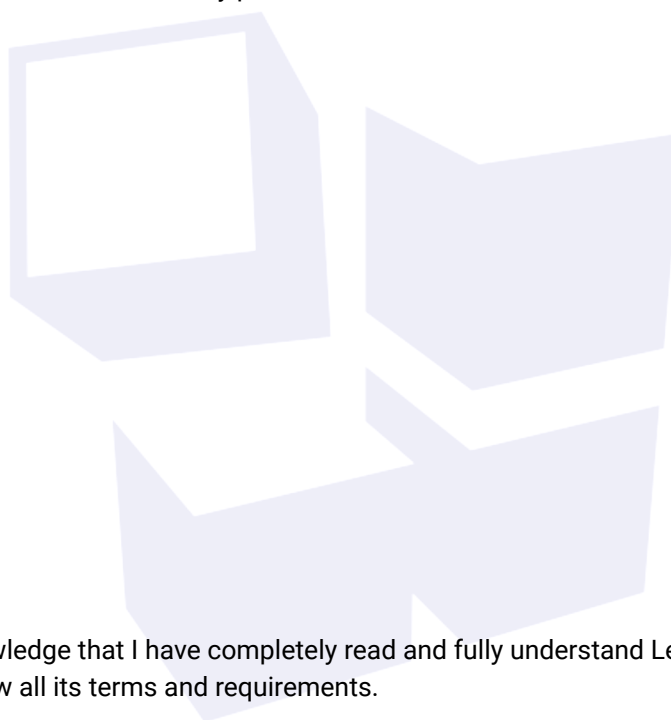
1942 Broadway St, STE 314C
Boulder, CO 80302

Audit, logging and enforcement

1. All activity within Level7's applications, systems, networks, servers and other devices may be logged and audited.
2. Violation of any terms of this policy may result in immediate termination of Level7's employee/contractor employment agreement or contract.
3. Any willful or malicious misuse, abuse or violation of this policy may result in criminal and/or civil penalties. Level7 reports all suspected criminal activity to the local law enforcement.

Issue Notification

Shall any employee/contractor observe any signs of an attempted or successful security breach, network intrusion, data theft, virus/malware infection, security policy violation or any other security concern, they are required to immediately notify Level7's IT admin or other designated Level7 security personnel.



By signing below, I hereby acknowledge that I have completely read and fully understand Level7's Information Security Policy outlined above and agree to follow all its terms and requirements.

Employee/Contractor's Signature:

Date:

Print name:

Phone

(877) 7-LEVEL7 (877-753-8357)
(720) 600-6202

Email & Website

L7.io
info@L7.io

Corporate Address

1942 Broadway St, STE 314C
Boulder, CO 80302