LEVIN SOURCES

Information Technology and Security Policy

1. Purpose

The purpose of this policy is to establish standards for the protection and security of all information held and processed by Levin Sources. Effective implementation of this policy will minimize the risk of loss or unauthorized access to Levin Sources and client information and technology.

This policy provides an overview of the systems and procedures that Levin Sources use to protect information. Individual aspects such as backup routines, password settings, remote access and encryption requirements are covered by separate policies.

2. Scope

This policy applies to all Levin Sources employees and systems. In addition to all associates and contractors that have a Levin Sources email address and access to our shared filing and systems.

3. Contents

A. Information Security Policy

1. Purpose

The purpose of this policy is to establish standards for the protection and security of all information held and processed by Levin Sources. Effective implementation of this policy will minimize the risk of loss or unauthorized access to Levin Sources and client information and technology.

This policy provides an overview of the systems and procedures that Levin Sources use to protect information. Individual aspects such as backup routines, password settings, remote access and encryption requirements are covered by separate policies.

2. Scope

This policy applies to all Levin Sources employees and systems.

3. Ethics and Acceptable Use Policies

Levin Sources expects all employees to conduct themselves in a professional and ethical manner. An employee should not conduct business that is unethical or illegal in any way, nor should an employee influence other employees to act unethically or illegally. Furthermore, an employee should report any dishonest activities or damaging conduct to an appropriate line manager.

Security of client information is extremely important to our business. We are trusted by our clients to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal information (i.e. - name, address, phone number, e-mail, Social Security number, bank account, credit card numbers, tax or income details, etc.) or company information not publicly available (i.e. – clients' financial information, employee information, accounts, technology, etc.). It is important that employees do not reveal sensitive information about Levin Sources or our clients to outside resources that do not have a need to know such information.

3.1. Protect Stored Data

Levin Sources will protect sensitive information stored or handled by the company and its employees. All sensitive information must be stored securely and disposed of in a secure manner when no longer needed for business reasons.

Access to the Levin Sources computer systems requires a username and password. Each user has a unique username and is given access to applications and data based on their business function. User accounts are managed by the Levin Sources outsourced IT department on instruction from the HR department. Employees leaving the company will have their access rights and permissions revoked at the earliest opportunity.

Any media (i.e - paper, floppy disk, backup tape, computer hard drive, etc.) that contains sensitive information must be protected against unauthorized access. This will include physical protection and, where possible, technological protection such as disk or file encryption.

Media no longer needed must be destroyed in such a manner to render sensitive data irrecoverable. This will include shredding of paper, physical destruction of tapes, compact disks, DVDs, and floppy disks, and secure wiping of hard disks.

Levin Sources will carry out routine backups of all client data held on the computer network. These backups will be tested regularly to ensure data can be recovered in case of loss on the live systems.

3.2. Protect Data in Transit

If sensitive information needs to be transported physically or electronically, it must be protected while in transit (i.e. - to a secure storage facility or across the Internet).

All Levin Sources portable computers (laptops) will be protected with full disk encryption. Levin Sources may also issue encrypted portable USB devices for the secure transfer of data. Transmission of sensitive data via the Internet shall only be via secure SSL transmission to recognized locations (such as transmission of tax information to HMRC).

3.3. Restrict Access to Data

To provide a high level of service, Levin Sources will regularly share information about clients within the organization. However, Levin Sources will restrict access to particularly sensitive information (business data and personal information such as payroll and personal tax details) to those that have a need-to-know.

3.4. Physical Security

Levin Sources will restrict physical access to sensitive information, and systems that house that information (i.e. computers or filing cabinets storing banking data), to protect it from those who do not have a need to access that information.

- Levin Sources will take appropriate security measures to protect their offices outside office hours, including alarm systems and, door locks.
- Access to all Levin Sources offices is protected by key access during office hours.
- Visitors should always be escorted and easily identifiable when in areas that may contain sensitive information.
- Password protected screen savers will be used on all computers that may contain sensitive information.

3.5. Personal use

Levin Sources provides computer equipment for usage associated with Levin Sources work.

- You are permitted, within reason, to use your laptop/desktop for personal communication and internet research outside of working time.
- Please do not use Levin Sources issued devices for illegal activities or personal entertainment / gaming / unauthorised downloads.

You may be subject to disciplinary action for any breaches of this policy (viewing pornography, violence, personal use in working time etc.)
As used in this policy, "working time" includes all time for which an employee is paid and/or is scheduled to be performing services for the Company. It does not include break periods, meal periods or periods in which an employee is not performing and is not scheduled to be performing services or work for the Company.

Where possible use of "own" laptops should be avoided to access company data, if it is necessary (due to failure of company laptop) you should work using Microsoft 365 and ensure all data is stored securely in the cloud and not on the laptop itself.

Longer term use of your own laptop must be approved by the Office Manager and our 3rd party IT Suppliers will need to ensure that you have adequate security in place.

3.6. Security Awareness and Procedures

Keeping sensitive information secure requires periodic training of employees and contractors to keep security awareness levels high. The following policies and procedures address this issue:

- Levin Sources will hold periodic security awareness training of employees and contractors to review correct handling procedures for sensitive information.
- Employees are required to comply with the Levin Sources Personal use policy.
- Background checks (such as criminal record checks, within the limits of local law) may be conducted where appropriate for employees that handle sensitive information.
- Levin Sources security policies will be reviewed and updated as needed.
- Levin Sources is Cyber Essentials certified and will re certify annually.

3.7. Security Management Incident Response Plan

There will be an employee of the company designated as the information security officer (ISO). The ISO / Office Manager is responsible for communicating security policies to employees and contractors and tracking the adherence to policies. In the event of a compromise of sensitive information, the ISO / Officer Manager will oversee the execution of the incident response plan.

Incident Response Plan

If a compromise is suspected:

- alert the information security officer / Officer Manger, who will alert 3rd Party IT provider 4Cambridge.
- 4Cambridge will conduct an initial investigation of the suspected compromise.
- If compromise of information is confirmed, the security officer will alert management and begin informing parties that may be affected by the compromise. Levin Sources will also act to contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.

4. Enforcement

Failure by an employee to comply with the standards and policies in this document may result in disciplinary action up to and including termination of employment.

B. Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Levin Sources' entire corporate network. As such, all Levin Sources employees (including contractors and vendors with access to Levin Sources systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

1. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any facility, has access to the Levin Sources network, or stores any non-public Levin Sources information.

3. Policy

- All administration passwords (e.g., root, enable, domain admin accounts, application administration accounts, etc.) must be changed from the installed default settings.
- All user-level passwords for access to the network must be changed at least every 90 days, be at least eight characters long, and not repeat any of the previous five passwords used.
- All user-level passwords must meet the complexity requirements and must contain at least 3 of the following: Uppercase characters (A through Z), Lowercase characters (a through z), Numbers (0 through 9), Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Password strength rules are set and enforced using Microsoft 365 settings and Active Directory Group Policies. These are set to be a password of at least 8 characters, with no maximum length, and complex passwords are enforced to stop the use of simple/common passwords. Microsoft 365 password are supported by MFA.
- Network administrators should use user-level accounts for all non-administrative tasks, and only use privileged administration accounts when required.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords should conform to the guidelines described below.

3.1. General Password Construction Guidelines

Passwords are used for various purposes at Levin Sources. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. (NOTE: Do not use either of these examples as passwords!)

3.2. Password Protection Standards

Do not use the same password for Levin Sources accounts as for other non-Levin Sources access (e.g., personal online email account, social networking sites, bank account access, etc.). Where possible, don't use the same password for various Levin Sources access needs. For example, select one password for your network user account and a separate password for individual applications.

We educate staff on good password setting and security behaviour using online training from KnowBe4. All employees complete the training, and this is tracked.

Do not share Levin Sources passwords with anyone, including IT or administrative staff. All passwords are to be treated as sensitive, confidential Levin Sources information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on holiday

If someone demands a password, refer them to this document or ask them to contact the IT Department.

Again, do not write passwords down and store them anywhere in your office. Do not store your passwords in a file on a computer system (including PDAs or smartphones) without encryption.

Change passwords at least once every three months.

If an account or password is suspected to have been compromised, report the incident to the Office Manager, and 4Cambridge immediately and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by 4Cambridge . If a password is guessed or cracked during one of these scans, the user will be required to change it.

3.3. Use of Passwords and Passphrases for Remote Access Users

Access to the Levin Sources Network via remote access is to be controlled using machine identification as well as a username and password. Anyone requiring remote access should contact the IT department for further guidance.

3.4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

C. Social Media Policy

At Levin Sources, we encourage you to use social media to interact with your colleagues and other sector players and to raise your profile as well as the company's. This can take the form of posts, tweets, comments, likes, shares, etc across any platform of your choosing.

However, this means that the line between professional and private can be blurrier in the digital space than it is in person. Even if you don't include Levin Sources in your bio or on your page, or you add a disclaimer, potential as well as existing clients can always find your social media handles and pass judgement on you and the company based on the content you share there.

This policy sets out guidelines on how social media should be used to support the delivery and promotion of Levin Sources, and the use of social media by the team in both a professional and personal capacity. It sets out what you need to be aware of when interacting in these spaces and is designed to help you support and expand our official social media channels, while protecting Levin Sources and its reputation and preventing any legal issues.

1. Point of contact for social media

The Marketing and Communications Specialist is responsible for the day-to-day publishing, monitoring and management of our social media channels. If you have specific questions about any aspect of these channels, or queries about how to best use your own social media platforms, speak to them.

2. What do we mean by "social media"?

The following list includes examples of social media platforms, but it isn't exhaustive:

- Twitter, Facebook, LinkedIn, Instagram, TikTok, Snapchat
- Messaging apps: WhatsApp, Telegram, Facebook Messenger, Signal
- Corporate social media: Skype, Slack
- This policy also covers blogs and personal websites

3. Social media platforms are part of your digital footprint

You are personally responsible for content published on your personal social media platforms, however, please be aware that existing, or potential clients, can always look you up, especially during the sales phase.

- The Internet doesn't forget. Although you can delete posts on most social media platforms, it could have been screenshot before, or a trace of it might remain.

- Use common sense and good judgement. Be aware of your association with Levin Sources and ensure your profile and related content is consistent with how you wish to present yourself to the general public, colleagues, partners, clients and funders.
- When in doubt, you can check with the Marketing and Communications Specialist (don't post).
- Be courteous in the way you express your opinions and disagreements. The debate level on social media can often stoop pretty low quite quickly; engaging with it at that level can be detrimental to both your reputation and mental health.

4. Protect Levin Sources

- Never disclose confidential or private information on social media platforms
- Avoid being critical of Levin Sources' clients or potential clients, even on your own social media accounts, even if you aren't directly working on that account!
- Keep an eye out for mentions of Levin Sources on social media, positive or negative. Send them to the marketing and communications specialist or share them on Skype
- Don't air personal grievance about projects, clients, Levin Sources or its staff on social media. Your line manager should be your first contact for this, alternatively you can speak with HR / Office Manager.
- Check with your colleagues or clients before posting any photo of them.

5. Differentiate your personal account from Levin Sources' corporate handles:

Be aware that any information you post, including on your personal social media channels, might affect people's perception of Levin Sources.

- Include a disclaimer on your social media platforms. Examples include:
    - Opinions are my own and not the views of my employer
    - My tweets are my own
    - My opinions are my own
    - The views expressed here are my own and don't necessarily represent Levin Sources' positions, policies or opinions.
- The disclaimer should be included:
    - Twitter: in the bio
    - Facebook: in the "about" section, "Details about you" subsection
    - LinkedIn: in the "about" section
    - Instagram: In the bio

However, please note that this disclaimer isn't full-proof and it won't stop a potential client from judging you/Levin Sources based on the content you have posted.

Senior management or those who are highly visible in their area of expertise must take particular care as personal views published may be misunderstood as expressing Levin Sources' view. (Even if you have a disclaimer)

If you run a personal blog or website which indicates in any way that you work at Levin Sources, you should discuss any potential conflicts of interest with your line manager.

6. Respect the law

Social media is regulated by the same laws as the rest of our lives. As such, you shouldn't post illegal content on it, including but not limited to:

- Never post content that is against the law. This includes, but isn't limited to, hate speech, threats of violence, discriminatory content, harassment, libel, etc.
- Posting copyrighted content without mentioning its authors and/or seeking their permission is also illegal.

7. Consequences of breach

Corrective counselling will be offered for minor indiscretions and where necessary, we will advise appropriate officials of any violations of law.

Any use of social networking sites that brings the Company into disrepute, or breaches the DE&I policy or harassment policy, will be regarded as gross misconduct and will result in dismissal.

D. Access Control Policy

The purpose of this policy is to confirm the access control policy, and how this is authorized and implemented.

1. User Account Creation

a) Every user has their own account with unique username and password for logging on to access business data.
b) New user form is prepared based on instructions and authorisation from the Office Manager.
c) These are then supplied to our outsourced IT provider for completion. User accounts are then created, and rights assigned based on the information supplied in the forms. User creation information is logged within the IT providers support system.

2. Leaver Accounts

a) When an employee leaves the organisation the Office Manager completes a leaver form and submits this to the external IT provider for actioning.
b) Their relevant service accounts are then disabled or deleted. Disabling or deletion of accounts is done using Active Directory to remove or disable the domain user account. This is then synchronised with the Microsoft 365 account to disable or delete as appropriate. If an account is cloud only then this is disabled or deleted directly within the Microsoft 365 admin console.

3. User Privileges

- User accounts on the domain and Microsoft 365 are created without any admin rights.
- User accounts within applications are based on job roles - so users get allocated the access rights and permissions based on their role.
- Changes to permissions and job roles are notified by the Office Manager to 4Cambridge , who then implements any required changes. The Office Manager completes a support request by email with 4 Cambridge, confirming the changes. These are then reviewed by 4Cambridge, who grants any additional permissions and removes any unnecessary permissions.

E. Administrative Access Policy

The purpose of this policy is to confirm who should be given administrative access, and how that is authorized and implemented.

1. Administrative Access

For the management of Levin Sources systems it is necessary for some staff to have administrative access to the network. This allows them to configure and manage the systems that are used by Levin Sources staff to carry out their duties.

Administrative access will include the following:

- Domain admin rights on the Active Directory network
- Administrator rights on the Office365 tenant (including Azure)
- Administrator access within Capsule
- Administrator access within Timesheet System Office
- Administrator access within Mendeley

2. Use of accounts with Administrative Access

Allowing an administrative account to access e-mail and browse the Internet makes it easier for attackers to introduce malware via a phishing attack or gain those credentials by using impersonation.

Accounts with administrative access (such as domain admin accounts) should therefore only be used for administrative tasks. Routine work, such as accessing email and web browsing, should be done with "normal" user accounts that do not have administrative access.

3. Granting Access

Administrative Access will be granted by approval from the Office Manager. The access will then be configured as required with the creation of user accounts with the appropriate rights.

4. List of staff with Administrative Access

At present the following staff are authorised for Administrative Access:

- Office 365 4Cambridge (outsourced IT provider)
- Active Directory 4Cambridge (outsourced IT provide)
- Capsule Office Manager and Managing Director
- Timesheet System Office Manager and Managing Director
- Mendeley Office Manager
- Citation Atlas Office Manager
- Home Office SMS Office Manager and Managing Director

F. Mobile Use and Data Access Policy

The purpose of this policy is to confirm Levin Sources use, management and security of all Mobile Devices that may access or hold company data.

1. Device Security

The mobile device should have the default security settings in place to protect the device. This would include automatic locking of the device after a set period, setting a passcode to unlock the device, and encryption must be enabled.
Any device should abide by the provider's application policy, so apps can only be installed from trusted sources (such as the Google Play store or Apple iStore). The devices should not be "rooted" or "jailbroken" to bypass this protection.
Any mobile devices must be kept up to date with the latest operating system and firmware from the manufacturer. We strongly recommend that automatic updates are enabled to achieve this.
Devices that are no longer supported by the manufacturer, or run on unsupported operating systems, are not permitted to access company data.

2. Permitted Apps

Staff are only authorised to access company data on mobile devices using the following applications:

- Outlook
- Teams
- OneDrive
- Word
- Excel
- PowerPoint
- The following web browsers: Google Chrome, Safari, Samsung Internet
- Timesheet System (via the app)

3. Reporting Loss or Theft

In the event of Loss or theft the user must act promptly to minimise the risk of compromise to company information by immediately:

- Reporting the loss to the Office Manager and 4Cambridge
- Changing any passwords that may have been used on the device.

Appropriate steps will be taken to ensure that company information on or accessible from the Mobile Device is secured, including remote wiping of the Mobile Device, where possible. Users should, therefore, regularly backup all personal data stored on the Mobile Device.

G. Revisions and Update

Revision and Updates				
Date	Approved by	Version	Changes	Signed
13/07/2023	Holger Grundel	2023 V1	Update of all policies Inclusion of sections on • Access Control Policy • Administrative Access Policy • Mobile Use and Data Access Policy To comply with requirements for Cyber Essentials Accreditation