Standard Security Procedures

All freelance and in-house employees at Localised Web S.L. have agreed to comply with the following security procedures:

- Safeguarding of content: I take care to prevent confidential project files and content from being accessed by unauthorized parties.
- No discussion: I do not discuss confidential project content with unauthorized parties.
- File deletion: I delete project files upon completion of work, or am willing to do so upon request.
- No paper copies: I either do not create paper copies, or am willing to agree to shred them upon project completion.
- Encrypted file storage: I understand how to, and am willing to agree to, store files only in encrypted form.
- Password-protected folders: I understand how to, and am willing to agree to, password-protect file folders.
- Encrypted file transfer: I understand how to, and am willing to agree to, send and receive project files in encrypted format.
- Dedicated project folder: I am willing to agree to keep separate file folders for separate clients.
- Remote backup: I have a regimen, available upon request, for backing up files remotely while work is underway.
- Archiving: I have a regimen, available upon request, for maintaining copies of project files after completion of work.
- No cloud storage: I am willing to agree to store content only locally on my own machine(s), i.e., not in "the cloud".
- No unauthorized sampling: I use samples from completed translations (in portfolios, or otherwise to market my services) only with client permission.
- Confidential collaboration: I do not disclose confidential information when obtaining assistance from fellow translators on term selection, etc.
- No term discussions: I am willing to agree not to obtain assistance from fellow translators on term selection, etc., at all.
- No ownership claims: I am willing to agree that completed translations are the property of the client or client's client, and waive any personal rights thereof.
- No foreign TM/MT: I am willing to agree not to use translation memories (TMs) or machine translation (MT) systems that contain data, or that have been trained using data, from other clients.
- Confidential TM/MT: I am willing to agree not to use content from projects worked on for one client, to add to translation memories or train MT systems that are used with other clients.
- TM/MT deletion: I am willing to agree to destroy any translation memories, machine translation engines and glossaries created specifically for a given project, upon completion of the project.
- No cloud MT/TM/etc.: I am willing to agree not to use any cloud-based translation memory, machine translation, optical character recognition (OCR) or other such cloud-based services that involve disclosure of content to third-party systems.
- No TM/MT sharing: I am willing to agree not to share a given client's TMs and MT training data with other professionals.
- Reference material confidential: I consider reference materials to be confidential; I do not share such materials, and would not use them on other client's projects, without permission.
- Dedicated computer: I have a dedicated computer for translation work.
- Locked computer: My work computer is password protected.
- Sole user: I am the only person who uses my computer.
- Antivirus: My computer has up-to-date, licensed antivirus software.
- File scanning: All incoming/outgoing files are scanned for viruses and malware.
- OS updates: Updates to my operating system are auto-installed.
- Software updates: I have a tool that checks for updates to all of the software on my computer.
- Anti-ransomware: I have an up-to-date, licensed anti-ransomware program.
- Private screen: My computer's screen is not visible through a window.
- Encrypted hard drive: My hard drive is encrypted.
- RAID: My hard drive(s) use redundant RAID.
- Locked phone: My mobile phone is pin or thumbprint protected.
- No pirating: I do not use pirated software.
- Anti-theft: My work computer has hardware anti-theft features.
- Password-protected network: My office's network is password protected.
- Firewall: My office's network is protected by a firewall.
- VPN: I understand how to, and am willing to agree to, use an encrypted VPN for file transfers.
- Encrypted email: I have an email account that enables me to exchange end-to-end encrypted messages, and am willing to agree to only such transfers.

Source: www.proz.com

Standard Security Procedures

- Non-disclosure of clients: I do not disclose my clients' identities or contact information, or the identities or contact information of their clients or vendors, without first obtaining permission to do so.
- Non-disclosure of processes, rates: I do not discuss my clients' internal processes, tools, rates of payment, or other such information, without first obtaining permission to do so.
- Private correspondence: I consider communications with clients to be confidential and do not disclose emails or other such correspondence.
- Secure record-keeping: My customer list(s), invoices and other such records are secured.
- Password management: I have a professional approach to passwords that involves (1) strong / long passwords; (2) different passwords for different sites/services; and (3) periodic password rotation.
- Two-step verification: I use of two-step verification procedures whenever possible.
- Conflict of interest: If I experience a conflict of interest, or recognize the possibility of that perception, I will immediately discuss that with my client.
- No privileged actions: It is my policy not to take any actions (ex. buying stock) as a result of having gained access to confidential information.
- Illegal activities: If I became aware of any illegal activity, it is my policy to immediately report that to the relevant authorities, and to my client if appropriate.
- Disclosure reporting: If confidential information were ever inadvertently disclosed, I would notify my client immediately.
- Code of conduct: I have either endorsed the ProZ.com Professional Guidelines (https://www.proz.com/professional-guidelines) or am bound by the code of conduct of a recognized industry association.
- Own NDA: I am able to provide my own NDA / security policy for clients who do not have one readily available.
- Assumption of confidentiality: Absent agreement to the contrary, my assumption is that files and content are to remain confidential.
- Experience with secure projects: I am experienced working with highly confidential content.
- Work on server: I am willing to agree to perform work remotely on tools/applications/portals controlled by the client.
- No subcontracting: I do not subcontract/outsource work, or I do not do so without client permission.
- Background check: I am willing to submit to personal background checks.

Security procedures available upon request

- No public spaces: I work exclusively, or almost exclusively, from my office.
- On-site audit: I am willing to agree to make my office available for on-site audit.
- File auditing: I understand how to, and am willing to agree to, enable security logging and file auditing.
- No outside Wi-Fi: I do not use, or am willing to agree not to complete a project using, Wi-Fi outside of my office.
- Wired connection: My network is wired; there is no Wi-Fi, or I am willing to agree to work only on a wired connection.
- Offline work: I am willing to work from my office, offline only, if required.

Source: www.proz.com