Security procedures - SecurePRO™ card

N. Groenendijk

Standard security procedures

- <u>Safeguarding of content</u>: I take care to prevent confidential project files and content from being accessed by unauthorized parties.
- <u>No discussion</u>: I do not discuss confidential project content with unauthorized parties.
- <u>Encrypted file storage</u>: I understand how to, and am willing to agree to, store files only in encrypted form.
- <u>Password-protected folders</u>: I understand how to, and am willing to agree to, password-protect file folders.
- <u>Encrypted file transfer</u>: I understand how to, and am willing to agree to, send and receive project files in encrypted format.
- <u>Dedicated project folder</u>: I am willing to agree to keep separate file folders for separate clients.
- <u>Remote backup</u>: I have a regimen, available upon request, for backing up files remotely while work is underway.
- <u>No cloud storage</u>: I am willing to agree to store content only locally on my own machine(s), i.e., not in "the cloud".
- <u>No unauthorized sampling</u>: I use samples from completed translations (in portfolios, or otherwise to market my services) only with client permission.
- <u>Confidential collaboration</u>: I do not disclose confidential information when obtaining assistance from fellow translators on term selection, etc.
- <u>No foreign TM/MT</u>: 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.
- <u>Confidential TM/MT</u>: 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.
- <u>No cloud MT/TM/etc.</u>: 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.
- <u>No TM/MT sharing</u>: I am willing to agree not to share a given client's TMs and MT training data with other professionals.
- <u>Reference material confidential</u>: 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.
- <u>Home office</u>: I have an office in my home.
- <u>Dedicated space</u>: My home office is in its own room.
- <u>Private space</u>: I am the only one who uses my home office.
- <u>No public spaces</u>: I work exclusively, or almost exclusively, from home.
- <u>On-site audit</u>: I am willing to agree to make my home office available for on-site audit.
- <u>Dedicated computer</u>: I have a dedicated computer for translation work.
- <u>Locked computer</u>: My work computer is password protected.
- <u>Sole user</u>: I am the only person who uses my computer.
- <u>Antivirus</u>: My computer has up-to-date, licensed antivirus software.
- <u>File scanning</u>: All incoming/outgoing files are scanned for viruses and malware.
- <u>OS updates</u>: Updates to my operating system are auto-installed.
- <u>Software updates</u>: I have a tool that checks for updates to all of the software on my computer.
- <u>Anti-ransomware</u>: I have an up-to-date, licensed anti-ramsomware program.
- <u>Private screen</u>: My computer's screen is not visible through a window.
- <u>Locked phone</u>: My mobile phone is pin or thumbprint protected.
- <u>No pirating</u>: I do not use pirated software.
- <u>Password-protected network</u>: My home office's network is password protected.
- <u>Firewall</u>: My home office's network is protected by a firewall.
- <u>No outside wifi</u>: I do not use, or am willing to agree not to complete a project using, wifi outside of my home office.
- <u>Wired connection</u>: My home network is wired; there is no wifi, or I am willing to agree to work only on a wired connection.

- VPN: I understand how to, and am willing to agree to, use an encrypted VPN for file transfers.
- 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.
- Security clearance: I currently hold an active security clearance from a governmental body.
- 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 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.
- 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.
- Drug testing: I am willing to submit to drug testing.
  Privacy is of the utmost importance to me. I use a VPN and my computers and home network are fully protected against malware and viruses. I only make back-ups on my private server, never in the cloud. All documents are treated confidentially. I never disclose my clients' name without permission. When I search the internet for terminology, I will never disclose proprietary names of products.

Security procedures available upon request
- 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.
- Archiving: I have a regimen, available upon request, for maintaining copies of project files after completion of work.
- 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.
- 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.
- File auditing: I understand how to, and am willing to agree to, enable security logging and file auditing.
- Offline work: I am willing to work from home, offline only, if required.
- Work on server: I am willing to agree to perform work remotely on tools/applications/portals controlled by the client.