Transcriber's Compliance Manual

Contents

Transcribers 2
PCs/laptops 2
Organising information security 3
Information asset management 3
Human resources security 4
Physical and environmental security 5
Communication and operations security 5
Logical access control 5
Information systems acquisition, development and maintenance 5
Information audit 5
Information security incident management 6
Continuity management 6
Compliance 6
Data Protection 7
Declaration 7

1. Transcribers

- All Transcribers are to sign and adhere to a legally binding Confidential Disclosure Agreement before commencing any work for and on behalf of McGowan Transcription. Transcribers may also be asked to sign further client or project-specific non-disclosure or similar agreements from time-to-time.
- Download all files (including but not limited to audio recordings, templates and discussion guides) using Sharefile, Global Lounge, Citrix system or a client's SSTP site where applicable.
- Once transcribed the audio recording must be deleted immediately using FileShredder software.
- When you upload transcripts to Sharefile/Global Lounge*, or email transcripts (but only upon prior written consent to do so) you do not need to encrypt you transcript unless instructed to do so. If in doubt, always use encryption.
- If your transcript does need to be encrypted the passwords must be at least 9 characters in length with a combination of alpha (upper and lower case) and numeric, and must be changed every month. McGowan Transcriptions will tell you what the passwords are for each new month. Passwords must be kept securely and never shared. Passwords must always be changed if there is suspected compromise.
- Once you have uploaded your transcript to whichever system is specified, then delete the transcript after 10 days using FileShredder software.

2. PCs/laptops

All Transcribers' PCs/laptops that are used to hold or process information received from McGowan Transcriptions must:

- Have a minimum standard operating system of Windows 7.
- Be maintained with the latest security patches issued by Microsoft.
- Be password protected; passwords must be to a minimum of 8 characters, using alphanumeric, with expiry no longer than 90 days. Inactive sessions shut down after 20 minutes and lockout after 5 failed attempts.
- Have access control implemented.
- Be protected against malicious code (viruses, spyware, Trojans) by use of properly installed and configured, reputable antivirus/anti spyware software. This software must be updated daily with the latest updates issued by the software vendor.

- Be protected by the use of an appropriate firewall, either incorporated within the router/modem or as a minimum a software firewall (e.g. provided with the anti-virus software). This must include intrusion detection protection.
- Where wireless network/internet connection is used the wireless router must be properly configured to ensure that only secure, authenticate wireless connections are permitted.
- All mobile computers that are used for downloading/transcribing material must be protected with full disc encryption, to at least a minimum of FIPS 140-2. We recommend either Windows BitLocker or VeraCrypt (https://www.veracrypt.fr/en/Home.html).

3. Organising information security

The person responsible for all Information Security is:

Joe McGowan – Managing Director
0800 158 3747 - 0790 880 9368
Joe@mcgowantranscriptions.co.uk

- Each member of McGowan Transcriptions must sign a legally binding Confidential Disclosure Agreement and this Compliance Manual before commencing work on any projects.
- Each Transcriber will hold a copy of their agreement and a scanned, signed copy to be uploaded to Global Lounge on an annual basis.
- Each Transcriber will read this Compliance Manual and show their agreement and compliance by filling in all relevant information required, and then signing and dating the last page annually.

4. Information asset management

- No transcripts must ever be printed or documentation taken out of your office or normal work environment.
- All electronic data must be encrypted if emailed (unless stated otherwise) (this must be at least 256bit AES encryption or similar).
- All transcripts must be encrypted before uploading them to the relevant directory on McGowan Transcriptions, Sharefile, Global Lounge, etc., unless stated otherwise in advance.
- You must not use removable media such as hard drives/memory sticks etc. to move data, and transcripts and recordings must be omitted from back-up systems ensuring that transcripts and

recordings are only on McGowan Transcriptions' systems 10 days after receipt.

- Our data deletion software is FileShredder v2 which adheres to US DoD (7 pass) standard. Please ensure you select '7 pass' when you install the software. www.fileshredder.org.
- McGowan Transcriptions prohibits the sharing or distribution of McGowan Transcriptions personal or confidential information.
- Should you at any point spot a possible security weakness it is your responsibility to inform McGowan Transcriptions immediately.
- Should you at any point breach any security requirements it is your responsibility to inform McGowan Transcriptions immediately. Thereafter you will be asked to complete and sign an Incident Report Form which you must do without delay.

5. Human resources security

The following documentation is required in hard copy for all Transcribers who work for McGowan Transcriptions:

- Identity validation (passport or photo driving licence with utility bill).
- Nationality and Immigration Status (copies of passport/driving licence and up to date copies of visas for those living outside of the UK).
- You must be a UK national and have an English bank account and pay tax (although you may reside outside of the UK).
- You must sign the tax confirmation document (separately attached) stating your tax reference.
- You will be fully trained to McGowan Transcriptions' standards before moving onto any high security government projects.
- The McGowan Transcriptions Confidential Disclosure Agreement clearly states the legal responsibilities with regards to confidential data and nondisclosure. Please ensure you are familiar with the terms of the document.
- You must have a current DBS Certificate.

McGowan Transcriptions reserve the right to require that criminal record checks (unspent convictions only) are carried out for members of the team working on certain projects.

6. Physical and environmental security

- Only authorised personnel should have access to McGowan Transcriptions client information; Citrix Safecodes and passwords must be kept in a secure area and only Transcribers who are members of the Senior team will be in possession of them.
- Should a Citrix safecode token be lost/stolen, it must be reported to McGowan Transcriptions immediately.
- Disaster recovery plans are not necessary for McGowan Transcriptions Transcribers as all recordings are stored on Citrix, Global Lounge and Sharefile.
- If you have a problem and have reason to believe you may miss a deadline on any project you must inform Joe McGowan and Julia Page immediately.

7. Communication and operations security

- Recordings from McGowan Transcriptions must never be used for any testing purposes.
- Your system must implement anti-virus measures and a firewall. Please note ALL the security software you have installed here:

8. Logical access control

Using our Sharefile/Global Lounge systems we can track who has uploaded or downloaded files. Each file is encrypted at source before going onto the Sharefile/Global Lounge System so there is no risk of data retrieval with unauthorised access.

9. Information systems acquisition, development and maintenance

By signing this document, you agree that access to all systems containing McGowan Transcriptions and its clients' information, in relation to maintenance or repair or replacement of equipment, is strictly controlled. This includes temporary access, either directly or indirectly, granted to engineers or external support services.

10. Information audit

As per point 7, our Sharefile system gives information on all of these factors.

- browsed information
- created information
- updated information
- deleted information

Our Global Lounge system also has a record of when the recordings were uploaded and transcripts received by the client. We have advanced reporting for each recording received, who it has been assigned to, when it was received by the Transcriber, when it is due back to McGowan Transcriptions, when it has been uploaded/downloaded and when it has been deleted from the system.

The audit trail on Sharefile/Global Lounge is checked regularly for all client projects and any unpredicted events will be investigated fully.

11. Information security incident management

Joe McGowan is responsible for handling security incidents within McGowan Transcriptions. If there is a security incident that is in breach of this document and/or our Information Security Policy it will be fully investigated and if deemed accidental then there will be one formal warning given, if breached a second time the Transcriber will no longer be able to work with McGowan Transcriptions.

If there is a security incident due to any of the specifications regarding security in this manual not being adhered to, the Transcriber will immediately cease working with McGowan Transcriptions.

12. Continuity management

In the event of a disaster that will affect any transcription projects or security, you must inform McGowan Transcriptions immediately via email or telephone.

13. Compliance

Joe McGowan is a member of the MRS and McGowan Transcriptions abides by their code of conduct. Your McGowan Transcriptions Confidential Disclosure Agreement adheres to this code of conduct.

No information must ever be passed to, or accessed by, a third party without Joe McGowan's specific authorisation.

14. Data Protection

Please be aware that voice recordings are considered personal data and therefore must be treated appropriately as per the Data Protection Act 1988. We have a separate policy in place with more information but you will find the general principles here. Please familiarise yourself with them and treat all voice files, templates, discussion guides and transcripts as personal data:

Please familiarise yourself with all areas of protecting personal data:

http://www.ico.org.uk/for_organisations/data_protection/the_guide/the_principles

http://www.ico.org.uk/for_organisations/data_protection/security_measures

Declaration

To be signed by all members of McGowan Transcriptions with access to information provided to by their clients.

A completed and signed copy of this Agreement must be uploaded annually to the 'Contracts' page on Global Lounge.

By signing below I confirm that I understand the responsibilities laid out in this Compliance Manual and that all work undertaken on behalf of McGowan Transcriptions will be undertaken to the principles and standards defined within this document.

Signature: _____

Name (in block capitals): _____

Date: _____

This document has a validity of one year only and must be resubmitted and signed on an annual basis.