Terms and Conditions, Privacy Policy & Information Security Management Policy

Contents

1 Terms and Conditions

1.1 Privacy

All therapy programmes are strictly confidential and undertaken in a professional, warm and caring manner. All personal information collected by CBT for You will be treated according to the principles of the Data Protection Act 1998.

Please refer to the privacy policy and information security management policy below.

1.2 Booking

To book or re-organise a therapy session:

- Fill out the online form;
- Email jane@cbtforyou.com;
- Call direct on 07514394941.

All therapy sessions are payable in advance at the time of booking (if booked on-line) or at the start of the session, unless funded through private medical insurance. Therapy sessions normally last for 50 minutes.

1.3 Cancellation & Rescheduling

No cancellations or rescheduling of appointments is permitted within 48 hours of the appointment time. Cancelled or rescheduled appointments within this time period will be charged at full rate.

Cancellations should be made by calling us on 07514394941.

If you are cancelling outside of normal opening hours (09:00 – 17:00), you may cancel by email but this should be followed up by telephone during opening hours.

If you have an email address registered with us, you will receive an email confirming your cancellation.

If the therapist is not available to deliver your appointment through circumstances beyond their control, we reserve the right to transfer the booking to an alternative date and time. In unusual circumstances we may need to cancel your booking. If we cannot fulfil your appointment, we will contact you by telephone, email or text – where possible.

1.4 Therapy Etiquette

Please arrive on time for all your appointments. If you do happen to be late, you will receive the remaining time for that session.

Please do not arrive early for an appointment as I do not have waiting room facilities and may still be in session with a previous client.

If a client arrives under the influence of alcohol, drugs or becomes abusive during the session, we reserve the right to cancel that session immediately & that session will still be charged for.

Notes may be taken during the session by the therapist, these are purely for the therapist's benefit (and private medical insurance company or therapy referral company where appropriate) only to support the work during the sessions and will remain the property & responsibility of the therapist throughout the sessions.

All Sessions are strictly confidential, however, if we hear of any harm to yourself, others, or the involvement of any illegal behaviour, then please note we are duty & legally bound to report this information to the relevant authorities, we will support you in that process.

Should you happen to see your therapist outside of your session time, your therapist will be happy to say hello, your association will not be disclosed & your sessions will not be discussed outside of therapy times.

1.5 Disclaimer

CBT for You do their utmost to ensure that the information contained on our website is both current and accurate. The information on the website must not be considered medical, legal or professional advice. We cannot therefore accept any responsibility for actions that arise from its use. The content of any pages referenced by an external link are not the responsibility of CBT for You.

1.6 Copyright

1.7 Links

This website contains links to other sites. CBT for You are not responsible for the privacy practices of such other sites. We advise that when you leave our site, to read the privacy statements of each website that collects personally identifiable information.

2 Privacy Policy

This privacy policy explains what personal data is, what types of personal data we collect, the purposes for which this data is collected as well as how it is processed, and what rights you have in this regard. You can rest assured that your personal data is handled with care.

2.1 What is Personal Data?

Personal data means any information relating to an identified or identifiable person, such as your contact information, payment history or your session data.

2.2 General Principles for Personal Data Processing

We adhere to the following principles when processing your personal data:

- We only collect personal data for specified, explicit and legitimate purposes (contact info, payment info, therapy status and progress);
- We do not collect personal data beyond what is necessary to accomplish those purposes;
- We will not use personal data for purposes other than that for which the data was collected;
- We will not transfer personal data to third parties, except in the case of private medical insurance companies from where the referral originated (where appropriate);
- We will do our best to ensure that information is up to date;
- We maintain appropriate technical and organisational measures to protect your personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing;
- Except when stated herein, we will not store personal data longer than is necessary to accomplish the purpose for which the data were collected or for which they are further processed, or as is required by law.

2.3 Personal Data we Collect and Process

We may collect and process the following data about you:

Data you give us. You may give us information about you by filling in forms on our site https://www.cbtforyou.com (our site) or by corresponding with us by phone, email or otherwise. This includes information you provide when you initiate contact to use our services (making a booking or discussing services prior to booking), request or receive consultation and initial and ongoing therapy. The information you give us may include your name, address, email address and phone number, financial and credit card information, personal info and medical history.

Data we receive from other sources. We may receive data about you from third parties we work closely with (including, without limitation, medical insurance companies, medical practitioners, business partners, sub-contractors, payment and delivery services, analytics providers, search information providers).

2.4 How we Use Your Personal Data

We use data held about you in the following ways:

Data you give to us. We will use this data:

- To carry out our obligations arising from any contracts between you and us relating to consultations and/or therapy, and to provide you with the information and services that you request from us;
- To provide you with information about other services we offer or other service providers that could assist you;
- To notify you about changes to our services;

Data we collect about you. We will use this data:

- To administer our service and for internal operations including delivering therapy, billing, scheduling therapy and liaising with private medical insurance companies who initiated such services.

2.5 Where we Store and Process Your Personal Data

Your personal data is stored and processed within the European Economic Area (EEA). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff may be engaged in, among other things, the processing of your payment details. By submitting your personal data, you agree to this transfer, storing or processing. In case of transfer of your personal data to any third countries, as defined in General Data Protection Regulation (GDPR), applicable legislation and regulations concerning such transfers are observed and relevant legal and security safeguards are ensured before such transfer.

All information you provide to us is stored on our secure IT infrastructure or paper record.

Transmission of information via electronic means to third part private medical insurance companies is executed using the method defined by that insurance provided and the insurance provider maintains full responsibility for the security of the data transfer mechanism and the data upon submission. Unfortunately, the transmission of information via the internet is not always completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

2.6 Our Disclosure of Your Personal Data to Third Parties

As a principle, we collect and process data only to facilitate the therapy sessions or improve the service you receive from CBT for You. We do not sell your personal data or share the said data with third parties, except to the extent stated in this Privacy Policy.

We may disclose your personal data to third parties to the extent required by law, court order or a decision rendered by a competent public authority and for the purpose of law enforcement. In addition, we may share your personal data with the following third parties:

- Private medical insurance companies responsible for initiating a programme of therapy for you at CBT for You;
- Third party vendors carrying out services on our behalf, including billing, sales, advertising, analytics, data storage, validation, security, fraud prevention, payment processing, and legal services. Such third-party vendors can perform these services but are prohibited from using your personal data for other purposes;
- Third parties to establish, exercise or defend legal rights of CBT for You;

- Third parties in the event of any merger, sale, joint venture, assignment, transfer or other disposition of all or any portion CBT for You assets (including without limitation in connection with any bankruptcy or similar proceedings);
- Other third parties subject to your consent.

In the event that we need to disclose your personal data to a third party, we take all reasonable steps to ensure that those third parties are bound by confidentiality and privacy obligations with respect to the protection of your personal data. The disclosure is conducted in compliance with legal requirements, including entering into data processing agreements with the relevant third parties, to ensure that personal data is only processed in accordance with our instructions, applicable law and regulations and for the purpose specified by us and to ensure adequate security measures.

2.7 Retention of Your Personal Data

In line with GDPR article 5 (e) that states all personal data shall be kept for no longer than is necessary for the purposes for which it is being processed and the requirement for retention associated to legal purposes, all personal data (including treatment records) will be destroyed upon seven years after completion of your treatment programme (discharge or date of last service). Data associated with minors will be deleted upon seven years after their 18th birthday following the date of discharge or date of last service.

Please refer to the information security management policy below.

2.8 Cookies

CBT for You does not use cookies, but some of our service provides (used for booking and payments) may use cookies and similar technologies like pixels, tags and other identifiers to remember your preferences.

A cookie is a small text file that is placed on your computer or mobile device when you visit a site, that enables us to: (1) recognise your computer; (2) store your preferences and settings; (3) understand the web pages you have visited; (4) enhance your user experience by delivering and measuring the effectiveness of content and advertising tailored to your interests; (5) perform searches and analytics; and (6) assist with security and administrative functions.

Pixels are tiny electronic tags with a unique identifier embedded in websites, online ads and/or email that are designed to: (1) collect usage information like ad impressions or clicks and e-mail open rates; (2) measure popularity of advertising; and (3) access user cookies.

As we adopt additional technologies, we may also gather information through other methods. Please note that you can change your settings to notify you when a cookie is being set or updated, or to block cookies altogether.

Please consult the “Help” section of your browser for more information. Please note that by blocking, disabling, or managing any or all cookies, you may not have access to certain features or offerings on our website.

2.9 Responsible for Processing

Dr Jane Ross is the CBT for You data controller and is responsible for the processing of your personal data.

YOUR RIGHTS

2.10 Access to Your Personal Data and Data Portability

You have the right to access the personal data concerning you which you have provided in a structured, commonly used format and have the right to transmit those data to any third party you should choose to.

Please refer to the information security management policy below.

2.11 Updating and/or Deleting Your Personal Data

We encourage you to update your personal data whenever there are changes in your personal data. Your personal data can be deleted unless we are obliged by applicable law and regulations to keep and process such information regardless of withdrawal of your consent. Following your request for deletion of your personal data, the data will be deleted from our records without undue delay; please note it may take a period of up to two (2) months to ensure complete deletion of any information stored in our back-up.

Please refer to the information security management policy below.

2.12 Right to Withdraw Your Consent

Some of CBT for You processing activities (scheduling and delivery of therapy) may be based on your consent. In these situations, you have the right to withdraw your consent at any time. Withdrawal of your consent will not affect the lawfulness of processing conducted prior to the withdrawal.

If you withdraw your consent, CBT for You and third parties involved in personal data processing will cease to process your personal data, unless and to the extent the continued processing or storage is required according to the applicable personal data legislation or other applicable laws and regulations. Please note that as a consequence of your withdrawal of your consent, CBT for You may not be able to meet your requests or provide you with our services.

Please refer to the information security management policy below.

2.13 Right to Complain

If you want to complain about a privacy breach, please contact CBT for You by sending your complaint to CBT for You, 32 Westburn Avenue, Inverurie, AB51 5QQ or by sending an e-mail to jane@cbtforyou.com.

We will acknowledge receipt of your complaint within five (5) business days. We will do our best to resolve it as quickly as possible and within one (1) month from the date of complaint. In case a response would require longer than one (1) month, we will let you know and inform you of the relevant reason(s).

If you are not satisfied with the outcome of your complaint or with our handling of your complaint at CBT for You, you may refer your complaint to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

MISCELLANEOUS

2.14 Third Party Websites, Plug-Ins and Services

The CBT for You website may contain links to third party websites. If you choose to use these websites or services, you may disclose your information to those third parties. CBT for You is not responsible for the content or practices of those websites or services. The collection, use, and disclosure of your personal data will be subject to the privacy policies of these third parties and not this Privacy Policy. We urge you to read the privacy and security policies of the relevant third parties.

2.15 Use by Children

CBT for You does not target and is not intended to attract children. Accordingly, our online services that collect personal data are not directed at and should not be accessed by individuals under the age of sixteen (16) years and we request that such individuals do not provide any personal data. Minors must obtain express consent from parents or legal guardians prior to accessing or providing any personal data. If notified by a parent or guardian, or discovered by other means, that a child under the age of sixteen has provided his or her personal data we will delete the child's personal data that is in our possession.

2.16 Changes to our Privacy Policy

We may modify or update this Privacy Policy when necessary to reflect changes in our products and services, changes in applicable legislation, regulations or practice and to address customer feedback. Accordingly, please review it periodically.

If there are material changes to this Privacy Policy, we will notify you either by posting a notice or by sending you a notification.

3 Information Security Management Policy Introduction

3.1 Introduction

The management of CBT for You, located at 32 Westburn Avenue Inverurie AB51 5QQ, which operates as a sole trader of cognitive behavioural therapy services, are committed to preserving the confidentiality, integrity and availability of all physical and electronic information assets throughout the organisation in order to preserve its legal, regulatory and contractual compliance. Information and information security requirements will continue to be aligned with CBT for You goals and the information security management policy is intended to be an enabling mechanism for information and data protection, for electronic operations, for e-commerce and for negating information related risk.

The information security management policy provides the context for identifying, assessing, evaluating and controlling information related risks through the establishment and maintenance of repeatable process and procedure. The Data Protection Officer is responsible for the management, maintenance and execution of the information security management policy.

In particular, business continuity and contingency plans, data backup procedures, access control to systems and information security are fundamental to this policy.

The information security management policy is subject to continuous, systematic review and improvement. The policy will be reviewed to respond to any changes in the risk assessment or risk treatment plans defined as a requirement of the GDPR.

3.2 Data Protection Info

Data Protection Officer: Dr Jane Ross

3.3 Rationale for a Data Protection Officer

Requirement for a DPO	Y/N	Comments
We are a public authority and have appointed a DPO (except if we are a court acting in our judicial capacity).	N	If yes, a DPO is required
Our core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.	N	If yes, a DPO is required
Our core activities consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.	N	If yes, a DPO is required

4 Article 30: Records of Processing Activities

Controller	Dr Jane Ross
Purpose of processing	All personal information is used to organise and process your therapy sessions, facilitate your use of our CBT for You, respond to your requests, and assist you with future use of our services. Maintenance of client details for the purpose of delivering Cognitive Behavioural Therapy including: • Initial consultation • Ongoing consultation • Reports to referring medical companies / organisations
Client categories	Personal data is held for all customers of CBT for You as part of delivering a suite of tailored therapy sessions.
Data categories	• Name • Address • DOB • Phone Numbers • Email • Referrer reference • Insurance reference • Method of payment • Insurance Provider • No of sessions approved • Price(s) per session • Invoice dates and numbers • Dates of sessions • Diagnosis • Difficulty • Questionnaires used & scores • Notes
Reason for data collection	Contact details are recorded and maintained for the sole purpose of scheduling therapy sessions. Session data is collected for the purpose of guiding therapy and providing feedback to the client as well as referring organisations.
Data recipients	At the request of referring private insurance companies and other therapy providers that have initiated the client's contact with CBT

	for You, we may be asked to deliver the following info: • Initial assessment • Ongoing assessment reports • Closeout reports All referring vendor requested reports are delivered using the mechanism prescribed by the vendor and the responsibility for the security and maintenance of that data is the vendors at the point of transfer. We will never rent or sell your personal information to any 3rd party.
Data retention	All personal therapy / session data (electronic and physical) held by CBT for You will be deleted after seven years of the completion of therapy. (seven years following the date of their 18th birthday for minors) Contact details are maintained in perpetuity to assist future engagement with CBT for You. Financial information is maintained for six years from the end of the financial year in which the transaction was made.
Security measures	All therapy session data is held on physical paper file during the execution of therapy sessions and shredded within 60 days of the completion of therapy – with ongoing retention for legal reasons via password protected electronic files. Client contact details are maintained on-line for the purposes of scheduling sessions. All personal information is used to organise and process your therapy sessions, facilitate your use of our CBT for You, respond to your requests, and assist you with future use of our services. Unless you opt out of receiving electronic reminders, we may send you information by email or text message about upcoming appointments to the contact details you provided.
Data stores	Physical paper file in secure cabinet. Set more scheduling database for contact details using HTTPS. Therapist personal computer (password protected). Network attached storage device for backup (password protected).

5 Risk Assessment

5.1 Scope

This method of risk assessment is applied throughout CBT for You in respect of all risks.

5.2 Responsibilities

The Data Protection Officer is responsible for carrying out risk assessments wherever they are required by the GDPR.

5.3 Identify the Risks

The risks to CBT for You's information are identified by the Data Protection Officer, covering availability, confidentiality and integrity.

The effect that losses of availability, confidentiality and integrity might have on CBT for You are identified.

Each risk is owned by the Data Protection Officer.

5.4 Assess the Risks

The impact that might result from the loss of availability, confidentiality or integrity, for each risk is assessed by the Data Protection Officer.

The realistic likelihood that each risk might occur is assessed.

The risk levels are subsequently assessed.

A decision is made, for each risk, as to whether it is acceptable or if it must be controlled in line with criteria established by the Data Protection Officer.

5.5 Risks Treatment

Each risk is analysed, and the appropriate action is assigned:

- Accept
- Reject
- Transfer
- Control

5.6 Control Objectives

Appropriate control objectives are selected or designed by the Data Protection Officer according to the specific needs of the risk and the organisation, and controls to achieve those objectives are selected from a variety of sources.

Controls are compared against the appendix to ensure that none have been missed.

6 Physical Entry Controls & Secure Areas

6.1 Scope

All designated secure areas of CBT for You's premises are subject to controlled access and usage.

6.2 Responsibilities

Every secure area has an owner and the owner is responsible for ensuring that prescribed controls are maintained.

All employees/ staff, contractors and third parties have certain responsibilities as defined below.

6.3 Procedure

Secure areas must be locked or occupied at all times.

Access to secure areas where confidential or restricted information is processed (including in conversation) or stored is restricted to authorised persons.

Authorisation is provided by the Data Protection Officer.

Access to secure areas requires authentication and authorised personnel are issued with pass codes or physical keys as appropriate.

The owner of a secure area is responsible for ensuring that no unsupervised access is provided to the secure area.

Third party support personnel only have access to secure areas when required and this access is specifically requested, authorised and monitored.

7 Retention of Records

7.1 Scope

All client and vendor details and information records, whether analogue or digital, are subject to the retention policy.

7.2 Responsibilities

The following roles are responsible for the retention of these records because they are the information asset owners:

The Data Protection Officer / GDPR Owner is responsible for the storage and subsequent deletion of data in line with this procedure.

7.3 Procedure

The required retention periods by record type are recorded in (Retention of Records – GDPR Rec 4.9) under the following categories:

- Record type
- Retention period
- Retention period start date (at creation, submission, payment, etc.)
- Retention justification
- Record medium
- Disposal method

For all storage media (electronic and hard copy records), CBT for You retains the means to access such data.

Access to stored data (electronic and hard copy records) is restricted solely to the Data Protection Officer.

8 Security Reports & Personal Data Breach Notification

8.1 Scope

This procedure applies in the event of a personal data breach under Article 33 of the GDPR – Notification of a personal data breach to the supervisory authority – and Article 34 – Communication of a personal data breach to the data subject.

8.2 Responsibility

All users (whether employees/staff, contractors or temporary employees/staff and third part users) are required to be aware of, and to follow this procedure in the event of a personal data breach.

All employees/staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer.

The Data Protection Officer is responsible for coordinating and managing the response to any reported weakness, event or incident, including documentation of all emergency steps taken, evidence collection, and closing out the event.

8.3 Notification (Data Processor to Data Protection Officer)

CBT for You reports any personal data breach or security incident to the Data Protection Officer without undue delay. These details are then subsequently recorded in the internal breach register (GDPR Rec 4.5). CBT for You provides the Data Protection Officer with all the details of the breach.

The breach notification can be made by email or phone call.

A confirmation of receipt of this information will be made by email.

The Data Protection Officer logs all information security and personal data reports immediately, allocating a unique number to each and uses this log to ensure that all reports are analysed and closed out.

All information security and personal data events, weaknesses and incidents are assessed and categorised immediately upon receipt. There are four categories: event, vulnerability, incident and unknown.

Events are occurrences that, after analysis, have no or very minor importance for information security or personal data.

Vulnerabilities are weaknesses that, after analysis, clearly exist as significant weaknesses compromising information security or personal data.

Incidents are occurrences of events that have a significant probability of compromising information security or personal data.

Unknowns are those reported events or weaknesses that, after initial analysis, are still not capable to one of the other categories.

Once an incident is contained and the required corrective action complete, the Data Protection Officer shall produce a summary of the incident, identifying the cause of the incident and analysing its progress, trying to identify how the organisation could have responded earlier or more effectively, or what preventative action might have been taken in advance, the effectiveness of the containment and corrective actions and the contingency plans, and how the incident was closed out.

8.4 Notification (Data Protection Officer to Data Subject)

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, CBT for You notifies those/the data subjects affected immediately.

The notification to the data subject describes the breach in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, CBT for You makes a decision based on assessment of effort involved in notifying each data subject individually, and whether it will hinder CBT for You's ability to appropriately provide the notification within a reasonable time frame. In such a scenario, a public communication or similar measure informs those affected in an equally effective manner.

8.5 Internal breach register

	Report prepared by:	
	Date:	
	On behalf of:	
1	Summary of the event and circumstances	
2	Type and amount of personal data	
3	Actions taken by recipient when they inadvertently received the information	
4	Actions taken to retrieve information and respond to the breach	
5	Procedures / instructions in place to minimise risks to security of data	
6	Breach of procedure/policy by staff member	
7	Details of notification to affected data subject Has a complaint received from Data Subject?	
8	Details of Data Protection training provided	
9	Procedure changes to reduce risks of future data loss	
10	Conclusion	

9 Right of Access

9.1 Purpose

Individuals have the right to access their personal data and supplementary information.

The right of access allows individuals to be aware of and verify the lawfulness of the processing.

9.2 Rights of Access 1

Individuals have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed;
- the period for which the personal data will be stored;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

9.3 Rights of Access 2

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

9.4 Rights of Access 3

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

9.5 Rights of Access 4

The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

9.6 Timescale and Charges

Any request for access to personal information will be provided without delay and at the latest within one month of receipt of request.

CBT for You will extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, CBT for You will:

- charge a reasonable fee taking into account the administrative costs of providing the information;

  or

- refuse to respond
- where CBT for You refuse to respond to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month

9.7 Information provision

CBT for You will verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, we will endeavour to provide the information in a commonly used electronic format.

10 Subject Access Request Form

The General Data Protection Regulations (GDPR) provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to see your data. You will also need to provide proof of your identity. Your request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

We will extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we will:

- charge a reasonable fee considering the administrative costs of providing the information; or
- refuse to respond.

Where we refuse to respond to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Proof of identity:

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of two documents such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The documents should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Administration fee:

Our policy is not to charge for Subject Access Requests unless the requests are manifestly unfounded or excessive (as above).

Section 1: Data Subject

Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title:	
Surname / Family Name:	
First Name / Forename:	
Date of Birth	
Address (inc. post code):	
Previous Address 1:	
Previous Address 2:	
Home Phone Number:	
Mobile Phone Number:	

I enclose the following copies as proof if identity:

Birth Certificate: ☐ Driving License: ☐ Passport: ☐ An official letter to my address: ☐

If none of these are available, please contact CBT for You for advice on 07514394941.

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require.

Details:

Section 2: Acting on Behalf of the Data Subject

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are NOT the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title:	
Surname / Family Name:	
First Name / Forename:	
Date of Birth	
Address (inc. post code):	
Previous Address 1:	
Previous Address 2:	
Home Phone Number:	
Mobile Phone Number:	

I enclose the following copies as proof if identity:

Birth Certificate: ☐ Driving License: ☐ Passport: ☐ An official letter to my address: ☐

If none of these are available, please contact CBT for You for advice on 07514394941.

What is your relationship to the data subject? (e.g. parent, carer, legal representative):

Relationship:

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

Letter of authority: ☐ Lasting or Enduring Power of Attorney: ☐

Evidence of parental responsibility: ☐ Other: ☐

If "other", please provide details: _____

Section 3: Declaration

Data Subject Declaration

I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that CBT for You is obliged to confirm proof of identity/authority and it may be necessary to obtain further information to comply with this subject access request.

Name: _____ Signed: _____ Date: _____

-or-

Authorised person – Declaration (if applicable):

I confirm that I am legally authorised to act on behalf of the data subject. I understand that CBT for You is obliged to confirm proof of identity/authority and it may be necessary to obtain further information to comply with this subject access request.

Name: _____ Signed: _____ Date: _____

Warning: a person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution.

I wish to:

Receive the info in electronic format: ☐

(some files may be too large to transmit electronically, and we may have to supply in CD format)

Receive the info by post*: ☐ Collect the information in person: ☐

View a copy of the information only: ☐ Review the info with a staff member: ☐

**Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.*

Please send your completed form and proof of identity to:

CBT for You, 32 Westburn Avenue, Inverurie, AB51 5QQ

jane@cbtforyou.com

CBT for You will retain the information provided and only share the information with those it is legally entitled to. The information will only be kept for as long as necessary and in accordance with CBT for You's retention policy, will be disposed of in a safe and secure manner.

11 Process for Consent

11.1 Scope

The consent of the data subject is one of the conditions for the processing of their personal data and is within the scope of this procedure. CBT for You needs to obtain consent when no other lawful basis applies.

Consent of the subject is defined in the GDPR as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Explicit consent is required for the processing of sensitive personal data. Specific conditions apply to the validity of consent given by children in relation to information services, with requirements to obtain and verify parental consent below certain age limits.

11.2 Responsibilities

As a data controller, CBT for You is responsible under the GDPR for obtaining consent from the data subject under advisement from the Data Protection Officer.

11.3 Consent Procedure

CBT for You provides a clear privacy notice wherever personal data is collected (GDPR REC 4.1) to ensure that consent is informed, and that the data subject is informed of their rights in relation to their personal data.

CBT for You demonstrates data subjects consent to the processing of his or her personal data or explicit consent for sensitive personal data (GDPR REC 4.6 – Data Subject Consent Form).

CBT for You demonstrates data subjects consent is intelligible and accessible using clear and plain language.

CBT for You demonstrates data subjects are informed of their right to withdraw consent before giving consent (GDPR DOC 2.7A – Right to Withdraw Consent Procedure).

11.4 Child Consent Procedure

Where processing relates to a child under 16 years old, CBT for You demonstrates that consent has been provided by the person who is the holder of parental responsibility over the child (GDPR REC 4.7).

11.5 Consent Best Practice

- We have made the request for consent prominent and separate from our terms and conditions
- We ask people to positively opt in
- We don't use pre-ticked boxes, or any other type of consent by default
- We use clear, plain language that is easy to understand
- We specify why we want the data and what we're going to do with it
- We give granular options to consent to independent processing operations
- We have named our organisation and third parties

- We tell individuals they can withdraw their consent
- We ensure that the individual can refuse to consent without detriment (albeit the process of scheduling appointments will become the responsibility of the client upon refusal)
- We don't make consent a precondition of a service

11.6 Recording consent

- We keep a record of when and how we got consent from the individual
- We keep a record of exactly what they were told at the time

11.7 Managing consent

- We regularly review consents to check that the relationship, the processing and the purposes have not changed
- We have processes in place to refresh consent at appropriate intervals, including any parental consents
- We make it easy for individuals to withdraw their consent at any time, and publicise how to do so
- We act on withdrawals of consent as soon as we can
- We don't penalise individuals who wish to withdraw consent

12 CBT for You Consent Form

CBT for You Consent Form & T&Cs

Your privacy is very important to me at CBT for You and I wish to continue communicating with clients in a way which is consistent with your expectations, and which is in line with UK data protection laws. Because of the introduction of the General Data Protection Regulations (GDPR) I now need your consent to continue contacting you regarding your ongoing treatment plan and appointments.

Here at CBT for You I will only use your personal information to administer your account and appointments and to provide the services you have requested from me. In line with GDPR article 5 (e) that states all personal data shall be kept for no longer than is necessary for the purposes for which it is being processed and for legal purposes, all personal data (including treatment records) will be destroyed after seven years upon completion of your treatment program or seven years following their 18th birthday for minors. Note, without formal consent I will be unable to contact you to arrange appointments and provide appointment reminders and the responsibility will fall to you to contact CBT for You for these purposes.

Please note that sessions cancelled with less than 48 hours' notice will be charged at the full amount. If you do not show up for a scheduled appointment, you will also be charged the full amount. This cancellation policy is standard in medical and mental health fields and will be strictly enforced. You will never be charged for a cancellation if it is made more than 48 hours in advance of your scheduled appointment time. Acceptance of the cancellation policy is implicit when making or accepting a booking with CBT for You. Please refer to the T&Cs at cbtforyou.com for more details.

By signing this form, you are confirming that you are consenting to CBT for You holding and processing your personal data for the purposes of keeping you informed about upcoming appointments and account management activities.

I consent to CBT for You contacting me by email and mobile regarding my appointments.

Name: _____ Signed: _____ Date: _____

Where you do not grant consent, I will not be able to use your personal data; (so for example, I may not be able to let you know about pending appointments); except in certain limited situations where required to do so by law. You can find out more about how I use your data from our "Information Security Management Policy" which is available from my website. You can withdraw or change your consent at any time by contacting CBT for You at 32 Westburn Avenue, Inverurie, AB51 5QQ or jane@cbtforyou.com. Please note that all processing of your personal data will cease once you have withdrawn consent, other than where this is required by law, but this will not affect any personal data that has already been processed prior to this point.

I am providing consent for a child under the age of 16:

Yes: ☐ No: ☐

If yes, please provide the full name of the child for which you are the legal guardian:

Child's Name: _____

Child's Age: _____

Your Relationship to the Child: _____

13 Revision History

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the GDPR. The current version of this document is available to all members of staff and clients of the organisation. It does not contain confidential information and can be released to all relevant external parties. This information security policy was approved the management of CBT for You on 11th May 2020 and is issued on a version-controlled basis under the control of the Data Protection Officer.

Name: Dr Jane Ross

Role: Data Protection Officer

Organisation: CBT for You

Date: 11-05-2020

Issue	Description of Change	Approval	Date of Issue
1.0	Initial release	Dr Jane Ross	01-05-2018
1.1	Update to reflect legal retention	Dr Jane Ross	11-05-2020

14 Appendices

14.1 Appendix 1: Controls and Objectives

A.5 Security policy

A.5.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Information security policy document

Control: An information security policy document shall be approved by management, and

published and communicated to all employees and relevant external parties.

A.5.1.2 Review of the information security policy

Control: The information security policy shall be reviewed at planned intervals or if significant

changes occur to ensure its continuing suitability, adequacy, and effectiveness.

A.6 Organisation of information security

A.6.1 Internal organisation

Objective: To manage information security within the organisation.

A.6.1.1 Management commitment to information security

Control: Management shall actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

A.6.1.2 Information security coordination

Control: Information security activities shall be co-ordinated by representatives from different parts of the organisation with relevant roles and job functions.

A.6.1.3 Allocation of information security responsibilities

Control: All information security responsibilities shall be clearly defined.

A.6.1.4 Authorisation process for information processing facilities

Control: A management authorisation process for new information processing facilities shall be defined and implemented.

A.6.1.5 Confidentiality agreements

Control: Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified and regularly reviewed.

A.6.1.6 Contact with authorities

Control: Appropriate contacts with relevant authorities shall be maintained.

A.6.1.7 Contact with special interest groups

Control: Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

A.6.1.8 Independent review of information security

Control: The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

A.6.2 External parties

Objective: To maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

A.6.2.1 Identification of risks related to external parties

Control: The risks to the organisation's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.

A.6.2.2 Addressing security when dealing with customers

Control: All identified security requirements shall be addressed before giving customers access to the organisation's information or assets.

A.6.2.3 Addressing security in third-party agreements

Control: Agreements with third parties involving accessing, processing, communicating or managing the organisation's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

A.7 Asset management

A.7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organisational assets.

A.7.1.1 Inventory of assets

Control: All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

A.7.1.2 Ownership of assets

Control: All information and assets associated with information processing facilities shall be 'owned' by a designated part of the organisation.

A.7.1.3 Acceptable use of assets

Control: Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

A.7.2 Information classification

Objective: To ensure that information receives an appropriate level of protection.

A.7.2.1 Classification guidelines

Control: Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation.

A.7.2.2 Information labelling and handling

Control: An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organisation.

A.8 Human resources security

A.8.1 Prior to employment

Objective: To ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

A.8.1.1 Roles and responsibilities

Control: Security roles and responsibilities of employees, contractors and third-party users shall be defined and documented in accordance with the organisation's information security policy.

A.8.1.2 Screening

Control: Background verification checks on all candidates for employment, contractors, and third-party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

A.8.1.3 Terms and conditions of employment

Control: As part of their contractual obligation, employees, contractors and third-party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organisation's responsibilities for information security.

A.8.2 During employment

Objective: To ensure that all employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.

A.8.2.1 Management responsibilities

Control: Management shall require employees, contractors and third-party users to apply security in accordance with established policies and procedures of the organisation.

A.8.2.2 Information security awareness, education and training

Control: All employees of the organisation and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.

A.8.2.3 Disciplinary process

Control: There shall be a formal disciplinary process for employees who have committed a security breach.

A.8.3 Termination or change of employment

Objective: To ensure that employees, contractors and third-party users exit an organisation or change employment in an orderly manner.

A.8.3.1 Termination responsibilities

Control: Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.

A.8.3.2 Return of assets

Control: All employees, contractors and third-party users shall return all of the organisation's assets in their possession upon termination of their employment, contract or agreement.

A.8.3.3 Removal of access rights

Control: The access rights of all employees, contractors and third-party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9 Physical and environmental security

A.9.1 Secure areas

Objective: To prevent unauthorised physical access, damage and interference to the organisation's premises and information.

A.9.1.1 Physical security perimeter

Control: Security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.

A.9.1.2: Physical entry controls

Control: Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

A.9.1.3 Securing offices, rooms and facilities

Control: Physical security for offices, rooms, and facilities shall be designed and applied.

A.9.1.4 Protecting against external and environmental threats

Control: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.

A.9.1.5 Working in secure areas

Control: Physical protection and guidelines for working in secure areas shall be designed and applied.

A.9.1.6 Public access, delivery and loading areas

Control: Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

A.9.2 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.

A.9.2.1 Equipment siting and protection

Control: Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

A.9.2.2 Supporting utilities

Control: Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

A.9.2.3Cabling security

Control: Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

A.9.2.4 Equipment maintenance

Control: Equipment shall be correctly maintained to ensure its continued availability and integrity.

A.9.2.5 Security of equipment off premises

Control: Security shall be applied to off-site equipment taking into account the different risks of working outside the organisation's premises.

A.9.2.6 Secure disposal or re-use of equipment

Control: All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

A.9.2.7 Removal of property

Control: Equipment, information or software shall not be taken off-site without prior authorisation.

A.10 Communications and operations management

A.10.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

A.10.1.1 Documented operating procedures

Control: Operating procedures shall be documented, maintained, and made available to all users who need them.

A.10.1.2Change management

Control: Changes to information processing facilities and systems shall be controlled.

A.10.1.3 Segregation of duties

Control: Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

A.10.1.4 Separation of development, test and operational facilities

Control: Development, test and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.

A.10.2 Third-party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.

A.10.2.1 Service delivery

Control: It shall be ensured that the security controls, service definitions and delivery levels included in the third-party service delivery agreement are implemented, operated, and maintained by the third-party.

A.10.2.2 Monitoring and review of third-party services

Control: The services, reports and records provided by the third-party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

A.10.2.3 Managing changes to third-party services

Control: Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

A.10.3 System planning and acceptance

Objective: To minimize the risk of systems failures.

A.10.3.1 Capacity management

Control: The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

A.10.3.2 System acceptance

Control: Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

A.10.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

A.10.4.1 Controls against malicious code

Control: Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

A.10.4.2 Controls against mobile code

Control: Where the use of mobile code is authorised, the configuration shall ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code shall be prevented from executing.

A.10.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

A.10.5.1 Information back-up

Control: Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

A.10.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

A.10.6.1 Network controls

Control: Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

A.10.6.2 Security of network services

Control: Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

A.10.7 Media handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.

A.10.7.1 Management of removable media

Control: There shall be procedures in place for the management of removable media.

A.10.7.2 Disposal of media

Control: Media shall be disposed of securely and safely when no longer required, using formal procedures.

A.10.7.3 Information handling procedures

Control: Procedures for the handling and storage of information shall be established to protect this information from unauthorised disclosure or misuse.

A.10.7.4 Security of system documentation

Control: System documentation shall be protected against unauthorised access.

A.10.8 Exchange of information

Objective: To maintain the security of information and software exchanged within an organisation and with any external entity.

A.10.8.1 Information exchange policies and procedures

Control: Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.

A.10.8.2 Exchange agreements

Control: Agreements shall be established for the exchange of information and software between the organisation and external parties.

A.10.8.3 Physical media in transit

Control: Media containing information shall be protected against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries.

A.10.8.4 Electronic messaging

Control: Information involved in electronic messaging shall be appropriately protected.

A.10.8.5 Business information systems

Control: Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

A.10.9 Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

A.10.9.1 Electronic commerce

Control: Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification.

A.10.9.2 On-line transactions

Control: Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

A.10.9.3 Publicly available information

Control: The integrity of information being made available on a publicly available system shall be protected to prevent unauthorised modification.

A.10.10 Monitoring

Objective: To detect unauthorised information processing activities.

A.10.10.1 Audit logging

Control: Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

A.10.10.2 Monitoring system use

Control: Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.

A.10.10.3 Protection of log information

Control: Logging facilities and log information shall be protected against tampering and unauthorised access.

A.10.10.4 Administrator and operator logs

Control: System administrator and system operator activities shall be logged.

A.10.10.5 Fault logging

Control: Faults shall be logged, analysed, and appropriate action taken.

A.10.10.6 Clock synchronization

Control: The clocks of all relevant information processing systems within an organisation or security domain shall be synchronized with an agreed accurate time source.

A.11 Access control

A.11.1 Business requirement for access control

Objective: To control access to information.

A.11.1.1 Access control policy

Control: An access control policy shall be established, documented, and reviewed based on business and security requirements for access.

A.11.2 User access management

Objective: To ensure authorised user access and to prevent unauthorised access to information systems.

A.11.2.1 User registration

Control: There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

A.11.2.2 Privilege management

Control: The allocation and use of privileges shall be restricted and controlled.

A.11.2.3 User password management

Control: The allocation of passwords shall be controlled through a formal management process.

A.11.2.4 Review of user access rights

Control: Management shall review users' access rights at regular intervals using a formal process.

A.11.3 User responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

A.11.3.1 Password use

Control: Users shall be required to follow good security practices in the selection and use of passwords.

A.11.3.2 Unattended user equipment

Control: Users shall ensure that unattended equipment has appropriate protection.

A.11.3.3 Clear desk and clear screen policy

Control: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

A.11.4 Network access control

Objective: To prevent unauthorised access to networked services.

A.11.4.1 Policy on use of network services

Control: Users shall only be provided with access to the services that they have been specifically authorised to use.

A.11.4.2 User authentication for external connections

Control: Appropriate authentication methods shall be used to control access by remote users.

A.11.4.3 Equipment identification in networks

Control: Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

A.11.4.4 Remote diagnostic and configuration port protection

Control: Physical and logical access to diagnostic and configuration ports shall be controlled.

A.11.4.5 Segregation in networks

Control: Groups of information services, users, and information systems shall be segregated on networks.

A.11.4.6 Network connection control

Control: For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.

A.11.4.7 Network routing control

Control: Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

A.11.5 Operating system access control

Objective: To prevent unauthorised access to operating systems.

A.11.5.1 Secure log-on procedures

Control: Access to operating systems shall be controlled by a secure log-on procedure.

A.11.5.2 User identification and authentication

Control: All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

A.11.5.3 Password management system

Control: Systems for managing passwords shall be interactive and shall ensure quality passwords.

A.11.5.4 Use of system utilities

Control: The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

A.11.5.5 Session time-out

Control: Inactive sessions shall shut down after a defined period of inactivity.

A.11.5.6 Limitation of connection time

Control: Restrictions on connection times shall be used to provide additional security for high-risk applications.

A.11.6 Application and information access control

Objective: To prevent unauthorised access to information held in application systems.

A.11.6.1 Information access restriction

Control: Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

A.11.6.2 Sensitive system isolation

Control: Sensitive systems shall have a dedicated (isolated) computing environment.

A.11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

A.11.7.1 Mobile computing and communications

Control: A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.

A.11.7.2 Teleworking

Control: A policy, operational plans and procedures shall be developed and implemented for teleworking activities.

A.12 Information systems acquisition, development and maintenance

A.12.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

A.12.1.1 Security requirements analysis and specification

Control: Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

A.12.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

A.12.2.1 Input data validation

Control: Data input to applications shall be validated to ensure that this data is correct and appropriate.

A.12.2.2 Control of internal processing

Control: Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

A.12.2.3 Message integrity

Control: Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

A.12.2.4 Output data validation

Control: Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

A.12.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

A.12.3.1 Policy on the use of cryptographic controls

Control: A policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A.12.3.2 Key management

Control: Key management shall be in place to support the organisation's use of cryptographic techniques.

A.12.4 Security of system files

Objective: To ensure the security of system files.

A.12.4.1 Control of operational software

Control: There shall be procedures in place to control the installation of software on operational systems.

A.12.4.2 Protection of system test data

Control: Test data shall be selected carefully and protected and controlled.

A.12.4.3 Access control to program source code

Control: Access to program source code shall be restricted.

A.12.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

A.12.5.1 Change control procedures

Control: The implementation of changes shall be controlled by the use of formal change control procedures.

A.12.5.2 Technical review of applications after operating system changes

Control: When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.

A.12.5.3 Restrictions on changes to software packages

Control: Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.

A.12.5.4 Information leakage

Control: Opportunities for information leakage shall be prevented.

A.12.5.5 Outsourced software development

Control: Outsourced software development shall be supervised and monitored by the organisation.

A.12.6 Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

A.12.6.1 Control of technical vulnerabilities

Control: Timely information about technical vulnerabilities of information systems being used shall be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

A.13 Information security incident management

A.13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

A.13.1.1 Reporting information security events

Control: Information security events shall be reported through appropriate management channels as quickly as possible.

A.13.1.2 Reporting security weaknesses

Control: All employees, contractors and third-party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

A.13.2 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

A.13.2.1 Responsibilities and procedures

Control: Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

A.13.2.2 Learning from information security incidents

Control: There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

A.13.2.3 Collection of evidence

Control: Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

A.14 Business continuity management

A.14.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A.14.1.1 Including information security in the business continuity management process

Control: A managed process shall be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity.

A.14.1.2 Business continuity and risk assessment

Control: Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

A.14.1.3 Developing and implementing continuity plans including information security

Control: Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

A.14.1.4 Business continuity planning framework

Control: A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

A.14.1.5 Testing, maintaining and reassessing business continuity plans

Control: Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

A.15 Compliance

A.15.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

A.15.1.1 Identification of applicable legislation

Control: All relevant statutory, regulatory and contractual requirements and the organisation's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organisation.

A.15.1.2 Intellectual property rights (IPR)

Control: Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

A.15.1.3 Protection of organisational records

Control: Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

A.15.1.4 Data protection and privacy of personal information

Control: Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

A.15.1.5 Prevention of misuse of information processing facilities

Control: Users shall be deterred from using information processing facilities for unauthorised purposes.

A.15.1.6 Regulation of cryptographic controls

Control: Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

A.15.2 Compliance with security policies and standards, and technical compliance

Objective: To ensure compliance of systems with organisational security policies and standards.

A.15.2.1 Compliance with security policies and standards

Control: Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

A.15.2.2 Technical compliance checking

Control: Information systems shall be regularly checked for compliance with security implementation standards.

A.15.3 Information systems audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

A.15.3.1 Information systems audit controls

Control: Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.

A.15.3.2 Protection of information systems audit tools

Control: Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.