Information Security Guidance

[CONFIDENTIAL]

This document is intended for all personnel contracted to LexisNexis UK or otherwise under NDA.

Do NOT distribute outside of LexisNexis UK before getting permission from LNUK Legal.

Last Updated
8th January 2013
V3b

Table of Contents

A) Foreword

i. This document sets out the company's guidance and usage regarding data, information, services and communications. The guidance should be applied to all company material.

ii. Failing to adhere to the guidance set out in this document may result in serious disciplinary action. In some cases, this may even result in dismissal.

iii. The information in this document is subject to:

- The Privacy and Electronic Communications (EC Directive) Regulations.
- The UK Data Protection Act.
- The (US) Sarbanes-Oxley [SOX] Act.
- Payment Card Industry Data Security Standards (PCI-DSS).
- Accepted Data Encryption Standards.
- Reed Elsevier policy.

iv. If your area of work involves:

- Information Technology.
- Product development.
- Project management of IT solutions or products.
- High levels of personal data manipulation and management (e.g. marketing databases).

… You should also read the "LNUK Product Information Security Guidance" document which supplies supplementary information.

B) What is Information Security?

i. Information security is the preservation of **confidentiality**, **integrity** and **availability** of information, regardless of the form it takes - digital or hard copy.

ii. Information must only be accessed by authorised people, kept accurate, complete, reliable and available when and where it is required.

iii. LNUK determines loss-impact potential by assessing the reputation, financial and operational impact to the company that may result from any realised risk to confidentiality, integrity & availability of information.

- **Confidentiality:** Prevent disclosure of information & data to unauthorised individuals / systems.
  - Can damage reputation, trust within the community, create legal claims.

- **Integrity:** Prevent undetectable or unauthorised modification of information & data.
  - Can impact decision making, force corrections or recreation of information.

- **Availability:** Ensure that information and data is accessible whenever it is needed.
  - Can mean information is not accessible and therefore halt processes.

iv. These 3 principles are used throughout this document and in particular in Section D – Media Security.

v. In order to secure and protect information, it is important to manage any risk by identifying.

- **Targets:** What are the information assets that need protection?

- **Threats:** Who or what do they need to be protected from?

- **Impacts:** What are the likely impacts if the protection fails?

C) Authorised access & use of company facilities

i. You may only make use of LNUK / RE / 3rd party facilities if you are authorised to do so by your manager. LNUK, RE and authorised 3rd party facilities include (but are not limited to):

- Terminals: computer desktops, laptops, notebooks, tablets, etc.
- Phone & fax: fax machines, desk phones, mobile phones, voice-mail, etc.
- Networks: LNUK, RE & other third party.
- Internet: web browsing, file sharing, e-mail, instant messaging, social, office, etc.
- Media: documents, CDs, DVDs, Blu-ray, tapes, hard disks, etc.

ii. Personnel may only access the personal information of other personnel with both line management director and Human Resources director approvals.

iii. Any use of LNUK / RE / 3rd party facilities unrelated to a specific business purpose should be considered "personal use".

a) Do not download, store or (re-)communicate materials (such as images, e-books / text, graphics) protected by copyright or intellectual property rights unless you intend to use these for private study or the terms & conditions of the site permit you to do so.

b) Do not download, store or (re-)communicate any materials that may be considered obscene, profane, defamatory, discriminatory, harassment, pornographic, malicious (gossip) or otherwise likely to cause offence to any person.

c) Commercial software is not owned and must be licensed by LNUK / RE / 3rd party for use. Do not copy, download, install or use any software without the express permission of the LNUK Chief Technology Officer or the RE IS Helpdesk. Comply with any other restrictions on use of software of which you are informed.

d) All confidential or sensitive communications should be marked "**[Confidential]**". Do not transmit or otherwise disclose confidential information or trade secrets to parties that are not under a Non-Disclosure Agreement (NDA).

e) Communications sent using LNUK / RE / 3rd party facilities are both logged and monitored. This is essential to:

- Ensure compliance with the terms of this policy and with regulatory procedures and legislation.
- Properly investigate security incidents.
- Detect unauthorised access & use of LNUK / RE / 3rd party facilities.
- Train, monitor and maintain effective standards of service.
- Access company communications & materials in your absence for authorised business purposes.
- Locate and retrieve lost materials in the event of disaster or failure.

f) Communications may be disclosed in any legal action in which LNUK, RE or a contracted 3rd party are involved. This includes communications that may appear to have been deleted – as copies may be held by recipients, on backup or may be reconstituted from other sources.

g) It is not recommended you use LNUK / RE / 3rd party facilities for personal use, however, should you opt to do so, ensure that any personal communications are clearly marked "Personal use".

- Keep personal use to a minimum (time spent and frequency).
- Do not let it impact your job performance / office working hours.
- Do not conduct any business – personal or otherwise – that is not the business of LNUK / RE.
- Ensure there is no negative impact on LNUK / RE / contracted 3rd party.
- Ensure any use is lawful.
- Apply the terms of this document.
- Misuse of business facilities may result in disciplinary action or dismissal.

iv. You are responsible for the security of all LNUK / RE / 3rd party facilities made available to you.

a) Do not allow LNUK / RE / 3rd party facilities to be used by any unauthorised person.

b) Do not grant access to LNUK / RE / 3rd party facilities without express authority.

c) Do not install malware, viruses, keyloggers, etc on any LNUK / RE / 3rd party facilities.

d) Only company authorised equipment may be connected to the LNUK / RE / 3rd party network (this includes remote access – e.g. via VPN software).

e) Ensure company assets assigned to you are maintained in line with on-going security practices.

f) Do not remove / copy company information to any non-company asset or facility.
- Do not copy company information to personal e-mail, cloud, HDD, USB, CD / DVD, etc.

v. LNUK / RE / 3rd party facilities providers may remove and / or periodically make copies of communications (including source / destination addresses) and the contents of authorised facility networks (including email, instant messaging, social network information, network drives, local hard drives, etc).

vi. Unauthorised access to LNUK / RE / 3rd party facilities or materials (including: “hacking”, “cracking”, “bugging”, “spoofing” and “phishing”), unauthorised modification of computer material and storage of illegal information are criminal offences.

vii. Be aware of the social engineering efforts to obtain information and confirm identities by:

a) Asking the person to provide their details.
- Use the Reed Elsevier Global Address List (GAL).
- Confirm a call-back phone number (must be GAL registered).
- Ask the person to spell their name.
- Ask the person for [] manager's name, [] director's name, [] 3 people who report to them.

b) Asking why they need the information.
c) Asking the person to use a company facility to source any information they need.
d) Asking who authorised the request and independently verifying the authorisation.
e) Withholding contact / personal / confidential information.
f) Ignoring name drops, efforts to pressure or intimidate.
g) Informing your manager about any requests that are not routine.

viii. Do not create nor use unauthorised infrastructure on company premises.
a) No ad-hoc Wi-Fi / hard-wire networks.
b) No ad-hoc peer to peer terminal systems.

ix. Please contact the RE IS Helpdesk on +44 (0)1483 257777 (or ext. 7777) if you need further clarification on this matter.

D) Media security

Media classifications

Label media with the appropriate Media Classification marking. Consider unmarked documents as **Confidential**.

Media Classification marking	Loss Impact Potential?	Meaning	NDA needed for 3rd parties?	Destruction	Security
Public Release	None	Information with no loss impact should be marked Public Release. e.g. This documentation may already be in the public domain.	No	• Use good judgement • Recycle	Use good judgement.
Confidential (or unmarked)	Indeterminate Loss Impact Potential [ILIP]	Information with an indeterminate loss-impact potential should be protected, but may be shared with 3rd parties under a Non-Disclosure Agreement. This may include information such as policies and guidelines or client personal data that is not sensitive.	Yes	• Secure waste • Cross-cut shred • Incinerate • Pulp • Degauss • Over-write • Destroy (sub cm)	• Lock paper in cabinet. • Prefer access control. • Use good judgement to encrypt.
Restricted	High Loss Impact Potential [HLIP]	Information with a high loss-impact-potential must be stringently protected and is not normally shared with 3rd parties. This may include information on mergers & acquisitions, strategy, patents & product related intellectual property.	Yes	• Secure waste • Cross-cut shred • Incinerate • Pulp • Degauss • Over-write • Destroy (sub cm)	• Lock paper in cabinet. • Always apply access control. • Strongly recommend encryption.
Special Control (or Attorney-Client Privilege)	High Loss Impact Potential [HLIP]	Information with a high loss-impact-potential must be stringently protected and is not normally shared with 3rd parties. This may include employee Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), Protected Health Information (PHI), Electronic Health Records (EHI).	Yes	• Secure waste • Cross-cut shred • Incinerate • Pulp • Degauss • Over-write • Destroy (sub cm)	• Lock paper in cabinet. • Ensure all pages state "Attorney-Client Privilege". • Always apply access control. • Always encrypt.

- Do not process / store / retain credit & debit card data.
- Consider using http://www.dban.org/ for multi-pass over-write of magnetic media.
- Review the appropriate Reed Elsevier Document Retention policy for how long to keep specific documents.
  - Audit and Risk
  - Compliance & Corporate Responsibility
  - Corporate
  - Corporate Development
  - Investor Relations / Corporate Comms
  - Legal
  - Tax
  - Environmental, Health & Safety
  - Facilities & Operations
  - Finance & Accounting
  - Governmental Affairs
  - Marketing & Public Relations
  - Payroll
  - HR - Benefits
  - HR - Labour & Employment
  - Insurance / Risk Management
  - Information Technology
  - Publishing
  - Purchasing

Data classifications

Personal Data Class	Cookie Law Class	Type of data / information collected and processed	Purpose for retention	Data Retention Period	Info Class	Encrypt?
PII: Public Public data	Not Applicable	Any information about an individual that may be deemed personal but is already available in the public domain or with consent may be published in the public domain.	To publish information about an individual with that person's consent - or if the information is already in the public domain (and can be proven to be).	**Infinity.** The information is classified as already in the public domain.	Public Release	Not needed
PII: Session Web Browser Session Data	Site Feature	• Unique / session identifier. • Session link. • Layout preferences. • Referrer, redirector, click stream. • Token identifier. • Server identifier. • Platform identifier. • Access information.	To identify an individual's browser session, to manage that session independently (and securely) and to enable the individual to specify certain unique preferences features.	**Up to 6 months** retention from last login / request.	Confidential	Not needed
PII: Marketing Marketing Data	Site Feature	Includes all "Public Data" and "Web Browser Session Data" data plus… • Customer / prospect account number. • Full name. • E-Mail address. • Direct mailing address. • Telephone numbers. • Fax number. • 3rd party data selling. • Preferences. • Order information. • IP address.	To hold an individual's basic profile. The profile - with the consent of the individual - may be used for analytics / trend analysis, may be used for marketing campaigns / mailings and may be sold on. All marketing and trend analysis is subject to suppression at the individual's request.	**3 Years** retention from last login / request.	Confidential	Use good judgement
PII: Tracking Third Party Tracking & Analytics Data	Tracking	Third party dependent but may include web browser session data and marketing data. Information is collected by third parties in line with their analytics and tracking policies.	To track user visits across a web site and gather analytics about this data to improve web sites.	**Third party dependent.** Information is retained by the third party in accordance with third party analytics and tracking policies.	Confidential	Use good judgement
PII: Finance Financial Data	Not Applicable	Includes "Marketing Data" plus… • Account / relationship record. • Financial record. • Order details. • Card payment indicators.	To manage an individual's account, any orders, money paid / owing (including payroll), complaints & customer service type requests.	**7 Years** retention from last payment.	Confidential	Encrypt bank account details
SPII: Sensitive Sensitive Personal Data	Not Applicable	Includes "Financial Data" plus… • Health, religion or racial. • National identity number. • HR employee information. • Client sensitive documentation. • Biometric information.	To manage sensitive personal information around health, holiday & attendance. (Prospective) employee HR info is included. Certain client confidential information may also be held for products (e.g. details of a last will & testament)	Where possible, **7 Years** retention from last payment or use. Certain information may be kept indefinitely or otherwise in relation to UK statutory law. For example, information relating to a last will and testament, pension information or a legal contract.	Special Control	Encrypt all

Financial & sensitive data

Where relating to an individual always treat the following as sensitive & encrypt.

i. Bank account holder name.
ii. Bank account number + sort-code (include id numbers from institutions such as PayPal & Google Wallet).
iii. National Insurance / identity number.
iv. Passport number.
v. DVLA license number.
vi. Any religious belief, racial or ethnicity related information.
vii. Any information around political opinion or trade union membership.
viii. Any physical / mental health / sex life related information.
ix. Any information related to a legal offence.

Use your judgement to encrypt databases.

Prefer to encrypt where any 2 or more of the following fields are retained together against a person's name.

- Phone number.
- Address / postcode.
- E-mail address.
- Last 4 digits of credit card PAN.
- Fax number.
- Credit card expiry date

This data is sometimes used for alternate authentication & password reset purposes by various parties.

Payment Card Industry Data Security Standard (PCI-DSS)

i. LNUK and RE are obliged to comply with the Payment Card Industry Data Security Standards (PCI-DSS) relating to handling of payment cards (credit / debit).

a) Payment card data is defined here as: The long card number (PAN), the cardholder name, the start & expiry dates, the security CVV number, the issue number and any data on the magnetic stripe or chip.

b) The LNUK Payment Gateway and Invoice Payment websites accept universal card types including Visa, MasterCard and American Express.

c) To ensure compliance with PCI-DSS, payment card data is only processed by Customer Service.

ii. Personnel should pay attention to the following tenets.

Do: Authorised personnel only	**Don't:**
1. Process payment card info as soon as it is presented.	1. Write down any payment card data. e.g. In a notepad.
2. Ensure Point of Sale terminals are masking / truncating payment card data on receipts (i.e. only last 4 digits).	2. Store any payment card data on computers or on any other endpoint devices - e.g. in an e-mail, on iPhone / iPad / laptop.
3. Ensure that any unprocessed paper containing payment card data is stored in a locked and secured safe overnight.	3. Permit unauthorised personnel to collect, access, retain or process payment card data.
4. If you're unsure, ask with LNUK Credit Control.	

iii. LNUK does not accept payment card data sent by e-mail, fax or by post.

a) Permanently delete any e-mail containing payment card details. Send a standard template response letter back to the sender stating that the e-mail has been destroyed and no card details have been retained. Do not respond with a copy of the sender's message (and card details).

b) Securely destroy any fax that contains payment card details (confidential waste / shredder).

c) Never forward or send any e-mail containing payment card data internally or externally.

d) Payment card details should not be posted to anyone in the business.

- If you receive any payment card details in the post, black out the payment card details using a pen or permanent marker before scanning / filing / storing the document.
- Contact & ask the customer to either shop online or telephone customer services to make a card payment.

e) If a customer calls by phone and wants to pay by card:-

- Ask the customer to "Please hold and wait to be transferred to the Customer Service department."
- Put the call on hold & transfer the customer to Customer Service at: +44 (0) 845 370 1234.

Media and asset retention

i. Lock away any media containing personal data in a safe.

- Prefer the use of a strong, large, fireproof safe for office use.
- The wooden desk drawer cabinets in offices may be defeated with a crowbar.

ii. Do not leave media and assets containing personal data on desks.

- Not for any period where you are away from your desk.
- Not overnight.
- Take laptops home with you.

iii. In all cases, securely dispose of media containing personal data.

- See the media classifications table.

iv. For backups…

- Ensure any backup facilities you use are functioning by exercising restore procedures periodically.
  - Especially if backups are being held off-site or with 3rd parties.
  - Practice disaster recovery at least annually.
- Backed up information is subject to RE document retention policy.
- Where the loss of a backup impacts on a business function, escalate to management and document a requirement for business continuity & disaster recovery.

E) User accounts & passwords

Practice for managing user accounts

i. Account names do not always need to be e-mail addresses. Protect your own information from leaking by registering original account names rather than e-mail addresses where possible.

ii. Do not store your personal information – or personal information belonging to any employee on any system or account unless it is necessary to fulfil a specific business purpose.

iii. You must have both line management director and HR director express written approval to access or apply LNUK staff personal data to any system.

iv. If you are responsible for any LNUK or RE system the following guidance applies to you in your role as a System Access Authoriser (SAA).

- LNUK & RE account creation.
    - Ensure you are logged as being the "System Access Authoriser" (SAA) with RETS or the relevant system-administrator responsible for your system.
    - Ensure that RETS / other system-administrators are aware of the need to contact you (or more senior – named - employees) to authorise any other personnel requesting access.
    - Design a "new starter form" specifying the permissions that other personnel may be allowed to request. (Ask with the RE IS Helpdesk for assistance with this if you need it).
    - Scrutinize any request for access carefully and make an effort to contact the employee requesting access (particularly if the request is for a subordinate).

- Account recertification and modification.
    - Ask RETS / other system-administrators to supply you with a full list of people with access to the system every month.
    - Review this user list for people with access that may have left LNUK, RE or an authorised 3rd party.
    - Notify RETS / other system-administrators ASAP:-
        - To change permissions where certain employees may have changed roles.
        - To remove access for anyone you believe has left.
        - To remove access for anyone who has not logged on to the system in 90 days.

- Account revocation.
    - Ask RETS / other system-administrators ASAP to revoke access to your system for anyone you know has left LNUK, RE or an authorised 3rd party.
    - Ensure that ALL 3rd parties using your system notify you as soon as their personnel:
        - Change roles.
        - Leave.

Use strong passwords

i. Create a different password for every service / website you use.

ii. Do not disclose your password(s) to anyone – whether in Reed Elsevier or otherwise. System-administrators and desktop support personnel should not need it.

iii. Do not use nor embed dictionary words (as per below) in your passwords. Well known words are often tested for by hackers. Do not convert words to other languages and do not use obvious sequences. Hackers are wise to password guidance and employ software specifically designed to crack passwords. **Examples taken from "worst password" lists**: ~~secret | password | monkey | princess | dragon | passwd | 1234 | football | iloveyou | baseball | trustno1 | test | ninja | sunshine | welcome | letmein | ashley | harley | 11111111 | mustang | michael | qwerty | 12345678 | abcdefgh | Password1 | master | shadow | Jordan | P455w0rd1 | Happy1Secret2Password3 | PassworddrowssaP | Password12345 | Password1Secret2Test3.~~

iv. Change each of your passwords at longest every 90 days.

v. Don't reuse passwords.

vi. Anywhere possible, use a mix of characters:

- E.g. Upper-case (A-Z), lower-case (a-z), numbers (0-9) & symbols ([~) (@ £ ?).

vii. You must use passwords that are at least 7 characters long to comply with RE policy.

viii. Consider using complex, generated passwords and prefer very long passwords that maximises the number of characters a service allows. A good resource is https://www.grc.com/passwords.htm

- Western applications typically allow up to 95 possible combinations per character, so a 63 character long password would create a very large key space of 95^63, i.e. virtually impossible to crack.

- Prefer very long passwords when encrypting files as they may be acquired by someone you did not intend. Hackers use software tools that can crack passwords encrypted with certain encryption schemes and a 7 character password is unlikely to remain safe.

- Consider using well-known software / hardware personal services to manage your passwords. Examples include:

✓	1Password	https://agilebits.com/onepassword
✓	PasswordSafe	http://passwordsafe.sourceforge.net
✓	KeePass	http://keepass.info/
✓	YubiKey	http://www.yubico.com/yubikey

✓ **Prefer storing passwords in your head or safely hidden away on your person, NOT in the cloud.**
✓ **Use these personal tools AT YOUR OWN RISK!**

- Consider using well-known "auto-destruct message" services such as:

✓ PrivNote – https://privnote.com/
✓ BurnNote - https://burnnote.com/
✓ **Consider other means for sharing passwords such as splitting a password into 2 chunks and using a different channel to send each piece.**
✓ **Use these services AT YOUR OWN RISK!**

ix. Multi-factor authentication may be classed as something you: KNOW. HAVE. ARE.

- If an application supports SMS or Phone Factor Authentication – strongly consider using it.
- Consider tying your user accounts to either your work mobile phone or your personal mobile phone.

x. Consider running a periodic check on your e-mail addresses against well-known public services to test if your e-mail accounts are known to have been hacked. **Use these services AT YOUR OWN RISK!**
   - https://pwnedlist.com
   - https://shouldichangemypassword.com

xi. Make sure you are not being monitored when you enter your password.

xii. Check your computer for physical hardware based key-logging devices before using it.

xiii. Check the URL for any web site you use and ensure any personal details (such as username and password) are being sent encrypted (over https). Check the SSL certificate hasn't been revoked.

xiv. Where supported, try and use an alternate (security) e-mail address to send password resets to.

   - Don't use an alternate security e-mail address as your main one to register for web sites / services.
     - This ensures that if your main e-mail address is compromised, a hacker issuing password resets on other sites shouldn't be able to reset passwords & gain control of those accounts.

   - Where sites ask for security questions to issue new passwords:
     - It may be the case that such security questions and the answers are stored unencrypted. Such security information may be quickly compromised and abused.
     - If possible, supply your own unique questions & fabricate unique, complex, password-like answers for the service.
     - It makes little sense to store accurate information that someone else might guess. If someone can acquire / guess the answer(s), your accounts may be compromised.

xv. Aim to improve your password(s) every time you reset them (every 90 days at least).

   - The password you used yesterday may not be considered secure today.

   - A HPC cluster of 25 AMD GPUs has been used to brute-force crack LM encrypted passwords (14 uppercase characters – as per Windows XP) in 6 minutes. A NTLM password could be cracked in 5.5 hours.

   - With some hashing algorithms, GPU based systems can cycle through tens of billions of guesses per second. Where compromised web-sites may use weaker password hashing algorithms (to encrypt your password), it is essential to ensure you password is long & strong.

F) Data encryption

- All ciphers / encryption schemes should now use 256 bits minimum & prefer 512 bits where possible.

- All electronic certificates should employ a minimum of 2048 bits.

- Prefer the use of AES encryption.
    - Never use: SHA1, DES, MD4, MD5, RC2, RC3 where these are offered by software applications.

- Personnel should ensure that all personal data transfers use network services employing encryption.
    - If you are working on product, refer to the LNUK Product Information Security Guidance document.

Use WinZip to encrypt confidential files

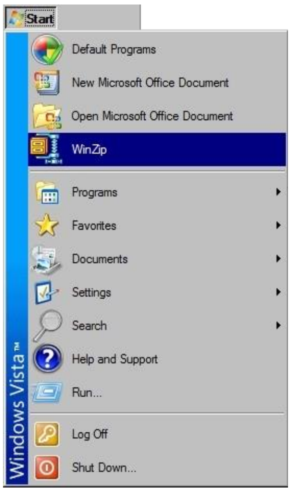
Step 1)

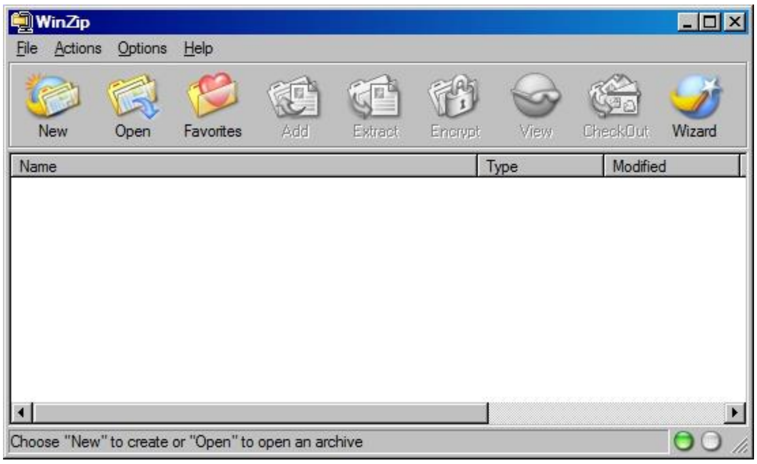
Start WinZIP.

- WinZIP should be installed on all LNUK desktops.

- If your machine does not have WinZIP installed, contact the RE IS Helpdesk.

- If using WinZip 10.0, use build 7245 or greater to avoid a known vulnerability in earlier builds.

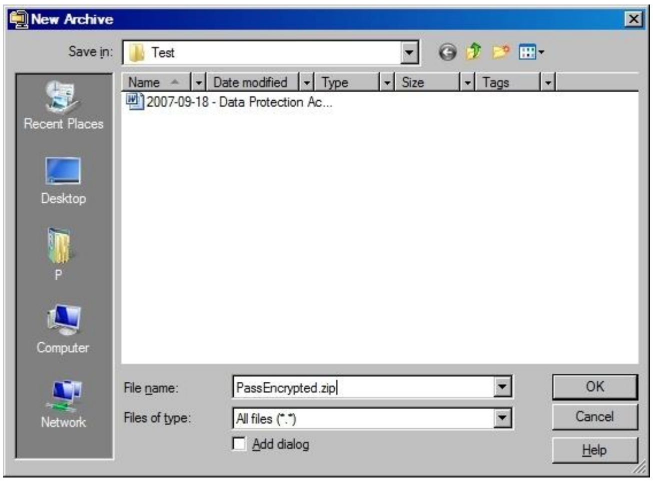




Choose "New" to create or "Open" to open an archive

Step 2)

- Click the "New" button on the toolbar & create a new Zip file (enter the filename & click OK).



File name: PassEncrypted.zip

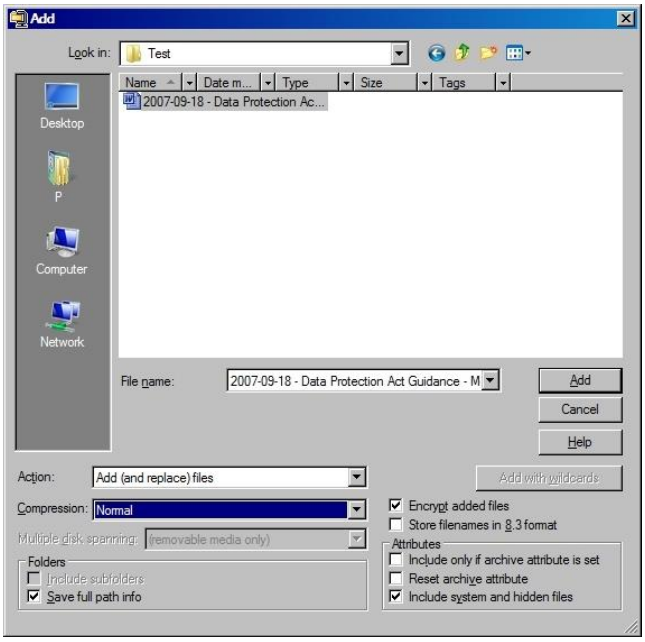
Files of type: All files (*.*)

□ Add dialog

Step 3)

Locate the files you want to add to the Zip file.

- Ensure you encrypt personal, sensitive, confidential, restricted and special control files.
- Select **"Add (and replace) files"** as the Action.
- Ensure the boxes **"Encrypt added files"** and **"Save full path info"** are checked.
- For the best compatibility, use **"Normal"** compression.
- Click Add.



Look in: Test

2007-09-18 - Data Protection Ac...

File name: 2007-09-18 - Data Protection Act Guidance - M

Action: Add (and replace) files

Compression: Normal

Multiple disk spanning: (removable media only)

Folders
□ Include subfolders
☑ Save full path info

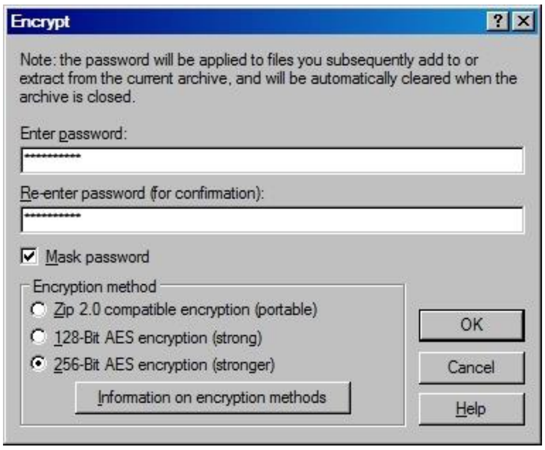
☑ Encrypt added files
□ Store filenames in 8.3 format

Attributes
□ Include only if archive attribute is set
□ Reset archive attribute
☑ Include system and hidden files

Step 4)

Select the **"256-Bit AES encryption (stronger)"** encryption method.

- Mask the password, then enter a unique strong password
- Click **"OK"**.



Note: the password will be applied to files you subsequently add to or extract from the current archive, and will be automatically cleared when the archive is closed.

Enter password: ***********

Re-enter password (for confirmation): ***********

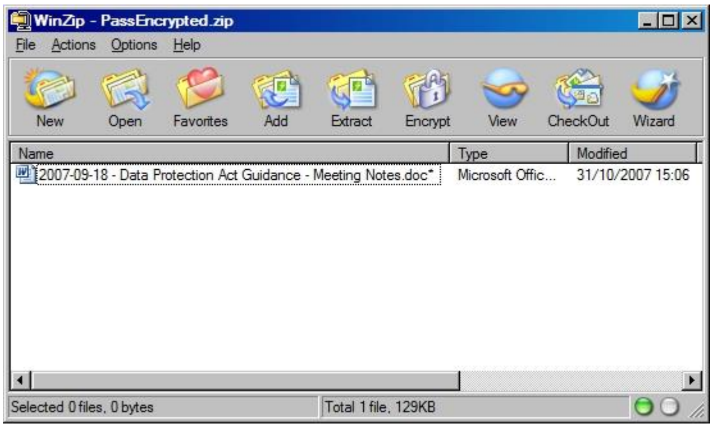
☑ Mask password

Encryption method
○ Zip 2.0 compatible encryption (portable)
○ 128-Bit AES encryption (strong)
● 256-Bit AES encryption (stronger)

Step 5)

You should now see your encrypted file(s) in the Zip you've created.

- Password protected files have an asterisk (*) next to them.
- You can now close WinZip.



Name	Type	Modified
2007-09-18 - Data Protection Act Guidance - Meeting Notes.doc*	Microsoft Offic...	31/10/2007 15:06

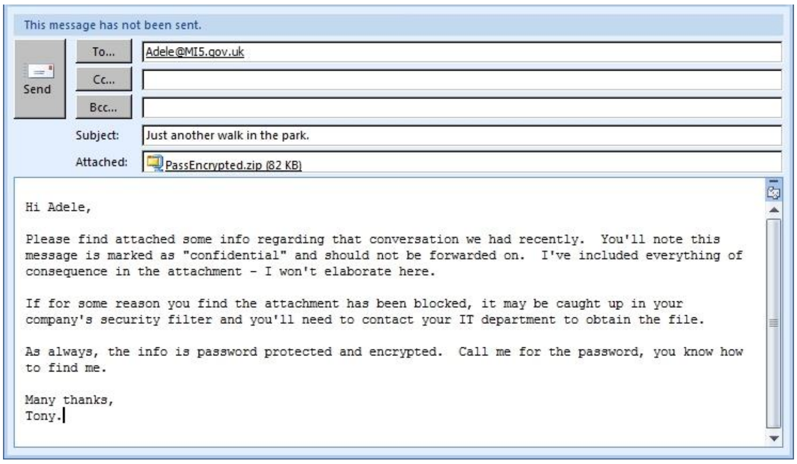
Selected 0 files, 0 bytes

Total 1 file, 129KB

Step 6)

You can now transfer / supply / transport the encrypted Zip file safely.

- Request that the recipient contacts you so that you may check you are giving the password to the intended recipient before giving out the password.
- Use a different communications channel to send a password compared with what was used to send the file.
- For example - by phone, by text message, by post, by cloud hosting solution - or - by e-mail (depending on the original method of transport).



This message has not been sent.

To... Adele@MI5.gov.uk

Cc...

Bcc...

Subject: Just another walk in the park.

Attached: PassEncrypted.zip (82 KB)

```
Hi Adele,

Please find attached some info regarding that conversation we had recently.  You'll note this
message is marked as "confidential" and should not be forwarded on.  I've included everything of
consequence in the attachment - I won't elaborate here.

If for some reason you find the attachment has been blocked, it may be caught up in your
company's security filter and you'll need to contact your IT department to obtain the file.

As always, the info is password protected and encrypted.  Call me for the password, you know how
to find me.

Many thanks,
Tony.
```

Use TrueCrypt containers to retain and encrypt confidential information

Advantages of using TrueCrypt

- Adds a layer of security to ensure cloud hosting providers, 3rd parties, hackers, governments, etc - cannot access your encrypted files.
- You manage the encryption and you decide which files warrant encryption.

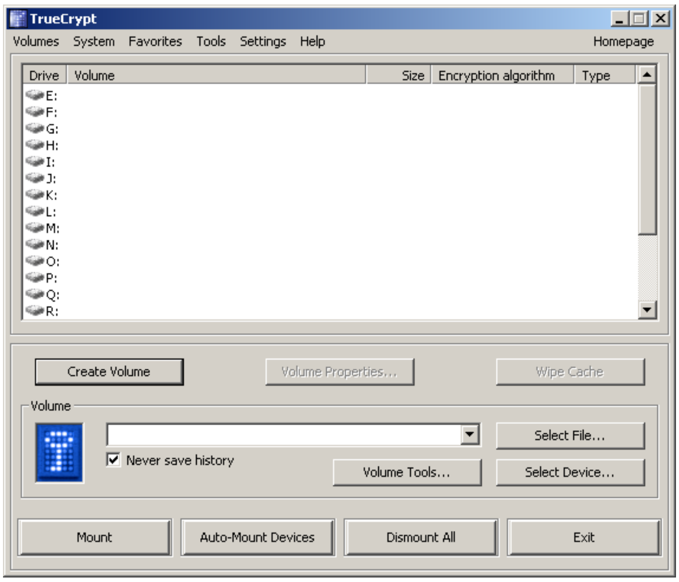
Also note:

- You will only be able to access your data where you can run TrueCrypt and it won't necessarily be easy to share encrypted volumes with others.
- Do not copy confidential information from a TrueCrypt container to any unencrypted area of a device as it will then be at risk of theft.
- Individual use (for secure backup / hosting files from a central location) is advised rather than sharing (it will prove to be easier to use WinZip to share encrypted files).
- Cloud based file hosting services - like Box.net - can create issues with sharing.
    - Expect file conflicts if you attempt to merge volumes between users.
    - Cloud hosting file sync status will only be on the container – not the files in it.
    - These services update the cloud copy at the bit / block level (reducing the amount of data that has to be uploaded for syncing). Large volumes will still take longer to sync as encrypted containers will show more changes. Try keeping individual containers to under 700MB in size.

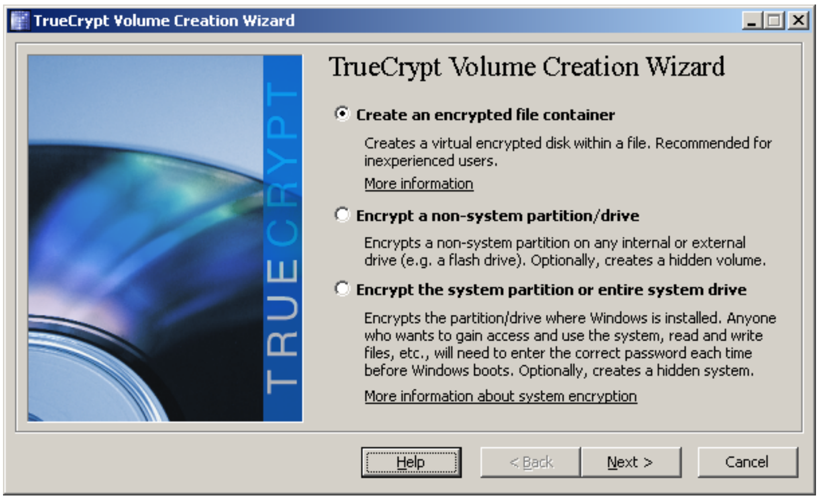
Setting up TrueCrypt

Step 1) Download, install and run the latest version *(at least 7.1a)* of TrueCrypt from www.truecrypt.org

Step 2) Click **"Create Volume"**.



Step 3) Select **"Create an encrypted file container"** then click **"Next"**.



TrueCrypt Volume Creation Wizard

● **Create an encrypted file container**

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ **Encrypt a non-system partition/drive**

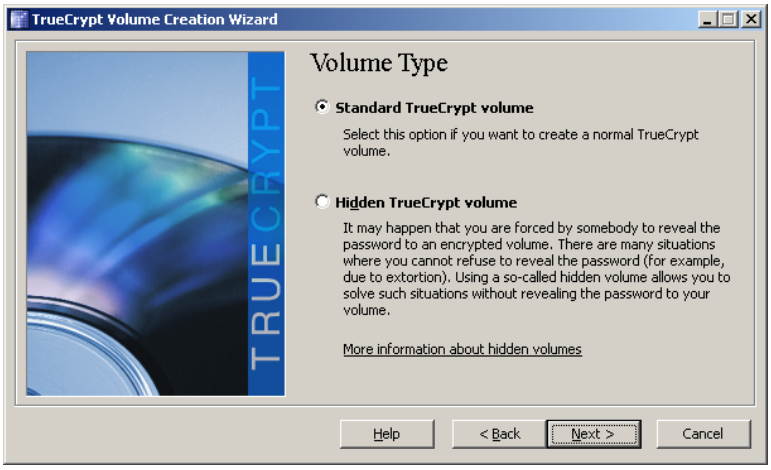
Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ **Encrypt the system partition or entire system drive**

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

More information about system encryption

Step 4) Select **"Standard TrueCrypt Volume"**, click **"Next"**.



Volume Type

● **Standard TrueCrypt volume**

Select this option if you want to create a normal TrueCrypt volume.

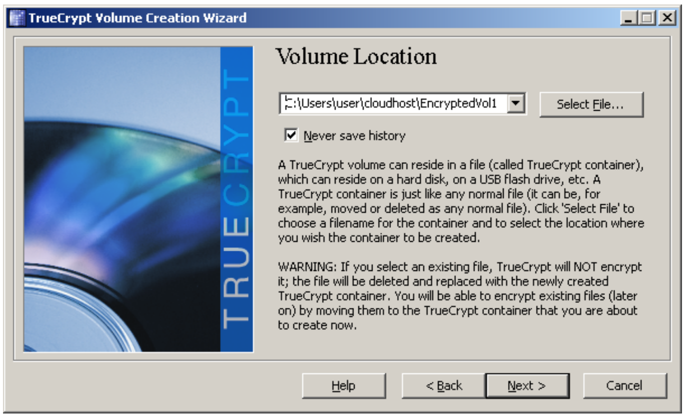
○ **Hidden TrueCrypt volume**

It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.

More information about hidden volumes

Step 5) Select a **"Volume Location"** for your TrueCrypt (*.tc) volume.

- Select the cloud hosting service folder on your local hard drive.
- Tick **"Never save history"** then click **"Next"**.



Volume Location

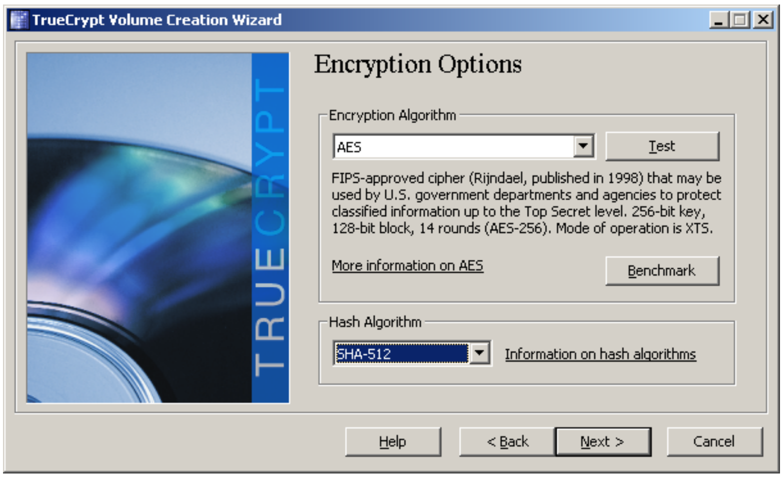
C:\Users\user\cloudhost\EncryptedVol1

☑ Never save history

A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.

Step 6) Select the **"AES"** Encryption Algorithm and **"SHA-512"** as the Hash Algorithm.



Encryption Options

Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

More information on AES

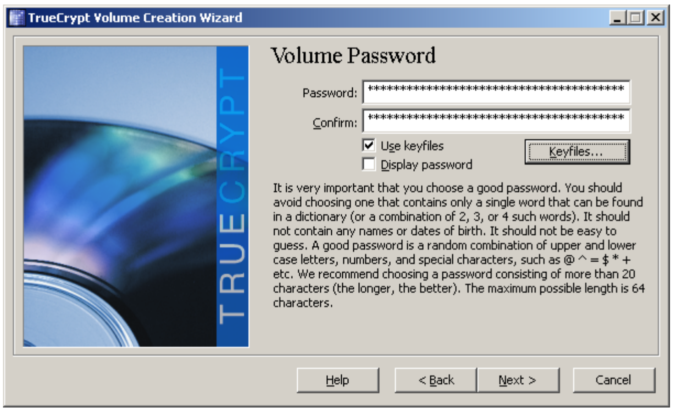
Hash Algorithm: SHA-512

Information on hash algorithms

Step 7) Select an appropriate Volume Size and provide a complex, strong password.

- Tick **"Use keyfiles"** and - if appropriate - click **"Keyfiles…"** to generate some Keyfiles.

- Sharing Keyfiles with users (e.g. using a USB memory stick) should allow teams to share a volume.



TrueCrypt Volume Creation Wizard

Volume Password

Password: **

Confirm: **

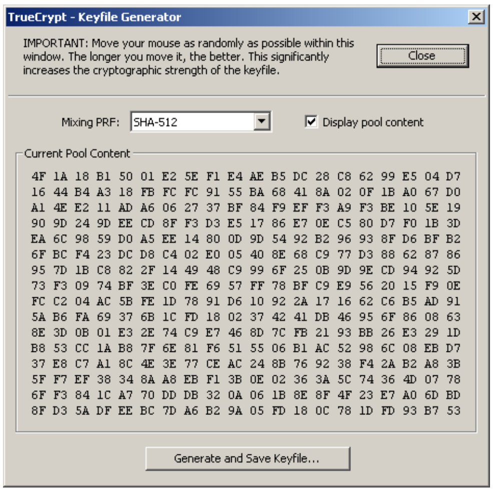
☑ Use keyfiles

□ Display password

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.

Step 8) Create a key file for the volume, clicking **"Generate and Save KeyFile"** to do this.

- Click **"Add Files"** to add the keyfile you just generated.
- Click OK and when you return to the **"Volume Password"** dialog - click **"Next"**.



TrueCrypt - Keyfile Generator

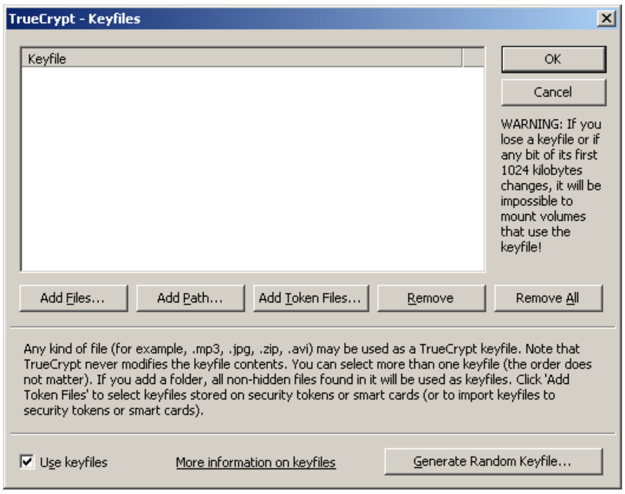
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the keyfile.

Mixing PRF: SHA-512

☑ Display pool content

Current Pool Content

```
4F 1A 18 B1 50 01 E2 5E F1 E4 AE B5 DC 28 C8 62 99 E5 04 D7
16 44 B4 A3 18 FB FC FC 91 55 BA 68 41 8A 02 0F 1B A0 67 D0
A1 4E E2 11 AD A6 06 27 37 BF 84 F9 EF F3 A9 F3 BE 10 5E 19
90 9D 24 9D EE CD 8F F3 D3 E5 17 86 E7 0E C5 80 D7 F0 1B 3D
EA 6C 98 59 D0 A5 EE 14 80 0D 9D 54 92 B2 96 93 8F D6 BF B2
6F BC F4 23 DC D8 C4 02 E0 05 40 8E 68 C9 77 D3 88 62 87 86
95 7D 1B C8 82 2F 14 49 48 C9 99 6F 25 0B 9D 9E CD 94 92 5D
73 F3 09 74 BF 3E C0 FE 69 57 FF 78 BF C9 E9 56 20 15 F9 0E
FC C2 04 AC 5B FE 1D 78 91 D6 10 92 2A 17 16 62 C6 B5 AD 91
5A B6 FA 69 37 6B 1C FD 18 02 37 42 41 DB 46 95 6F 86 08 63
8E 3D 0B 01 E3 2E 74 C9 E7 46 8D 7C FB 21 93 BB 26 E3 29 1D
B8 53 CC 1A B8 7F 6E 81 F6 51 55 06 B1 AC 52 98 6C 08 EB D7
37 E8 C7 A1 8C 4E 3E 77 CE AC 24 8B 76 92 38 F4 2A B2 A8 3B
5F F7 EF 38 34 8A A8 EB F1 3B 0E 02 36 3A 5C 74 36 4D 07 78
6F F3 84 1C A7 70 DD DB 32 0A 06 1B 8E 8F 4F 23 E7 A0 6D BD
8F D3 5A DF EE BC 7D A6 B2 9A 05 FD 18 0C 78 1D FD 93 B7 53
```



TrueCrypt - Keyfiles

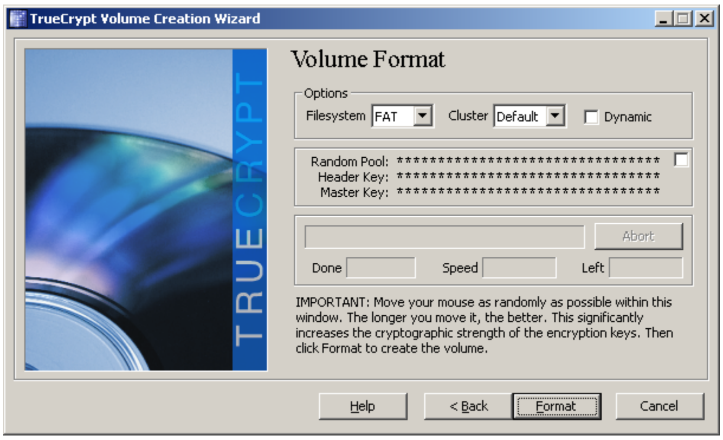
Keyfile

WARNING: If you lose a keyfile or if any bit of its first 1024 kilobytes changes, it will be impossible to mount volumes that use the keyfile!

Any kind of file (for example, .mp3, .jpg, .zip, .avi) may be used as a TrueCrypt keyfile. Note that TrueCrypt never modifies the keyfile contents. You can select more than one keyfile (the order does not matter). If you add a folder, all non-hidden files found in it will be used as keyfiles. Click 'Add Token Files' to select keyfiles stored on security tokens or smart cards (or to import keyfiles to security tokens or smart cards).

☑ Use keyfiles

Step 9) Select the FAT file system then click **"Format"** to format the volume.



TrueCrypt Volume Creation Wizard

Volume Format

Options

Filesystem FAT

Cluster Default

□ Dynamic

Random Pool: ******************************** □

Header Key: ********************************

Master Key: ********************************

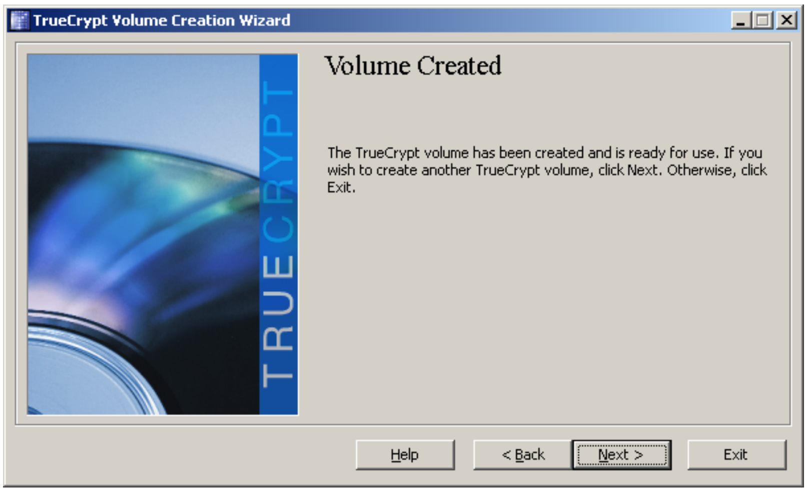
Done

Speed

Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Step 10) When the volume is formatted, you can now click **"Exit"**.

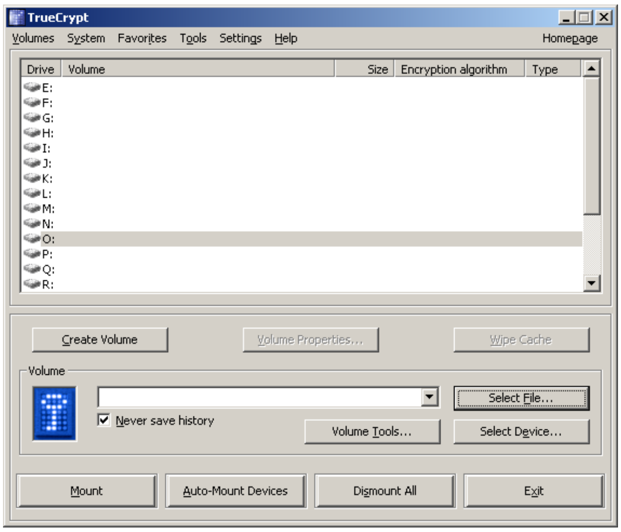


Volume Created

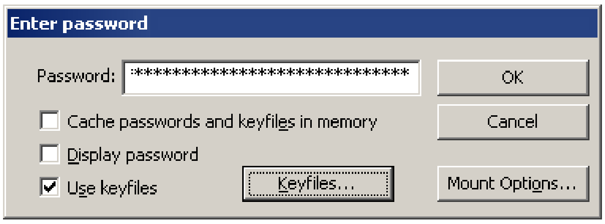
The TrueCrypt volume has been created and is ready for use. If you wish to create another TrueCrypt volume, click Next. Otherwise, click Exit.

Using TrueCrypt

Step 1) Open TrueCrypt and click **"Select File"**. Locate your TrueCrypt (*.tc) volume.



Step 2) Click **"Mount"**, then enter the volume password and **"Use keyfiles"**.
Select the keyfile for the volume. Click **"OK"** to mount.



Enter password

Password: ******************************

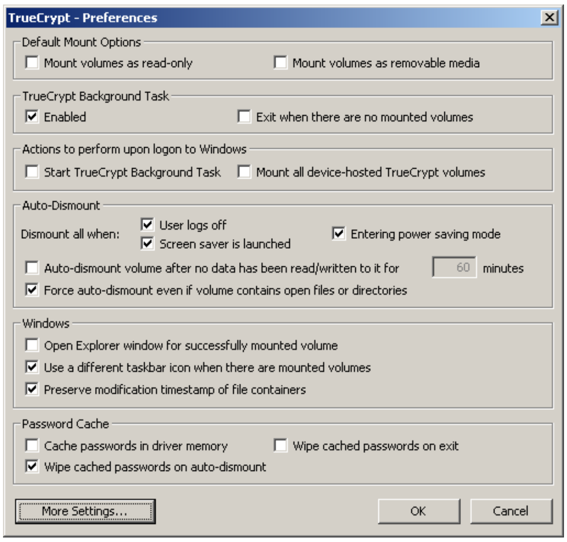
□ Cache passwords and keyfiles in memory

□ Display password

☑ Use keyfiles

Step 3) From the **"Settings"** menu - select **"Preferences"**.

- In the popup, locate the section **"Auto-Dismount"** and ensure **"Entering power saving mode"**, **"Screen saver is launched"** and **"Force auto-dismount even if volume contains open files or directories"** are ticked.
- Click **"OK"** to store these security settings.



TrueCrypt - Preferences

Default Mount Options
□ Mount volumes as read-only □ Mount volumes as removable media

TrueCrypt Background Task
☑ Enabled □ Exit when there are no mounted volumes

Actions to perform upon logon to Windows
□ Start TrueCrypt Background Task □ Mount all device-hosted TrueCrypt volumes

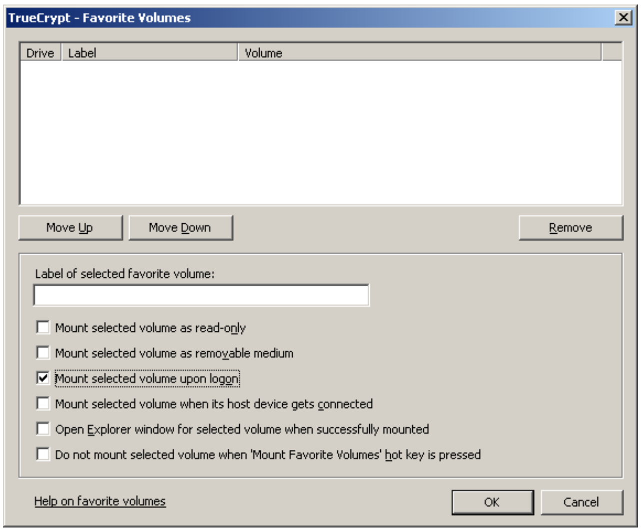
Auto-Dismount
Dismount all when: ☑ User logs off ☑ Screen saver is launched ☑ Entering power saving mode
□ Auto-dismount volume after no data has been read/written to it for 60 minutes
☑ Force auto-dismount even if volume contains open files or directories

Windows
□ Open Explorer window for successfully mounted volume
☑ Use a different taskbar icon when there are mounted volumes
☑ Preserve modification timestamp of file containers

Password Cache
□ Cache passwords in driver memory □ Wipe cached passwords on exit
☑ Wipe cached passwords on auto-dismount

Important note: Auto-dismounting is essential in case someone steals your computer. Dismounting removes your encryption key from system memory preventing container encryption keys being isolated & retrieved by Direct Memory Access (DMA) or physical freezing. Keep in mind that open application files are unencrypted in memory. For this reason it is wise to disable system hibernation & prefer to shut down your computer when you are not using it. Be sure to check your computer for rogue devices (e.g. key-loggers) if it has been left unattended for any period of time.

Step 4) From the **"Favourites"** menu, select **"Add Mounted Volume to Favourites"**.
Ensure **"Mount selected volume upon logon"** is ticked. Click **"OK"**.



Label of selected favorite volume:

- ☐ Mount selected volume as read-only
- ☐ Mount selected volume as removable medium
- ☑ Mount selected volume upon logon
- ☐ Mount selected volume when its host device gets connected
- ☐ Open Explorer window for selected volume when successfully mounted
- ☐ Do not mount selected volume when 'Mount Favorite Volumes' hot key is pressed

Any files you copy to this drive letter will be encrypted.

G) Data security incidents

- Contact the LNUK Security Incident Response Team (SIRT) immediately when you are aware of a security incident or data security breach.

- Supply the SIRT team member with:
  1. Your details (name, role, physical location).
  2. Date and time the incident took place.
  3. The nature of the incident.
     - What has happened and are there any losses?
     - What people / applications / systems / media / buildings are known to have been affected?
     - Were there any witnesses?
     - Any actions taken so far.
     - Be sure to specify if any personal data (as per specified in this document) is involved.

- The SIRT is on-call 24/7 to respond to security incidents.

Role	Contact	Tel (For 24/7 response)	E-Mail address
3rd Party management	Phil Garland	+44 (0) 7771 975698	phil.garland@lexisnexis.co.uk
IT & Operations	Neil Cuthbertson	+44 (0) 7920 862398	neil.cuthbertson@lexisnexis.co.uk
Finance	Lutz Kleinrensing	+44 (0) 7827 280439	lutz.kleinrensing@lexisnexis.co.uk
Legal	James Harper	+44 (0) 7833 040389	james.harper@lexisnexis.co.uk
Privacy & Comms	Emma Butler	+44 (0) 7795 315451	emma.butler@lexisnexis.co.uk

- LNUK SIRT members should follow up the incident.

H) Data Protection statement

i. LexisNexis Group and Reed Elsevier may process and retain any Personally Identifiable Information (PII) or Sensitive Personally Identifiable Information (SPII) you supply as a result of your employment in accordance with and as defined by the UK Data Protection Act. This includes information relating to your health, disabilities, racial and / or ethnic origin, trade union membership, etc. The purpose for this information collection is to enable LexisNexis Group and Reed Elsevier in complying with its contractual and non-contractual obligations, including without limitation: equal opportunities monitoring, sickness and absence monitoring, managing ill-health, incapacity issues and disability requirements.

ii. To the transfer of any PII or SPII retained and relating to you to any LexisNexis Group or Reed Elsevier Group company and their employees, professional advisors and third-party service providers, to HM Revenue & Customs and / or other authorities and prospective purchasers of any part of LexisNexis Group's or Reed Elsevier Group's business in exchange for suitable confidentiality undertakings – including transfers outside the European Economic Area subject to such transfers being made on the basis of a contract between a LexisNexis Group or Reed Elsevier Group company and the transferee which incorporates the model clauses published by the International Chamber of Commerce even where the territory in question does not maintain adequate data protection standards or, in the case of transfers to any LexisNexis Group or Reed Elsevier Group company outside the European Economic Area, subject to any implemented Binding Corporate Rules.

iii. To submit to additional background checks which the Company may reasonably request from you. These may be the same checks which you agreed to on commencement of your employment, or further checks - should business needs, legal or regulatory obligations mean that additional checks become advisable.

iv. You are entitled to update your information at any time and you are entitled to a copy of records LexisNexis and Reed Elsevier hold about you. Submit a Subject Access Request to the LNUK Data Protection Officer to source this information - see http://www.lexisnexis.co.uk/privacy/

I) Terminology

- **"Access authoriser" and / or "Data owner":**
  The person who is responsible for allowing others to access the system and its data. This is typically the product sponsor / owner.

- **Data controller:**
  A person (or people) who determines the purposes for which and the manner in which any personal data is, or is to be processed.

- **Data processor:**
  A person (or people) other than an employee of the data controller who processes the data on behalf of the data controller.

- **Data sub-processor:**
  A person (or people) other than an employee of the data controller / data processor who further processes the data on behalf of the data processor with the consent of the data controller.

- **Data subject:**
  An individual who is the subject of personal data.

- **Media:**
  Any material which may retain information.
    - e.g. Paper, CDs / DVDs / Blu-ray, cassettes / tapes, USB thumb drives, hard drives, etc.

- **Personal data or "Personally Identifiable Information" [PII]:**
  This is data which relates to a living individual who can be identified from:

    - (i) The data.

    - (ii) Other information that the data controller possesses or is likely to obtain… and includes any expression of opinion about the living individual and any indication of the intention of the data controller or any other person in respect of the individual.

- **Sensitive personal data or "Sensitive Personally Identifiable Information" [SPII]:**
  This means personal data consisting of information as to:

    - The racial or ethnic origin of a data subject.

    - Political opinions.

    - Religious beliefs or other beliefs of a similar nature.

    - Trade union membership (within the meaning of the Trade Union and Labour relations Act 1992).

    - Physical, mental health or condition.

    - Sexual life.

    - The commission or alleged commission of any offence and any proceedings / disposal of proceedings or court sentence thereof.