PremiumTrust Bank

PremiumTrust Bank

Procedure for the Management of Removable Media

Classification: Internal
April 2023
Document Number: PTB/ISMS/PMRM/A7.14

Status: APPROVED

Document Control Sheet

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
April 3, 2023	1.0	Document creation	Information & Cyber Security

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Contents

1. Introduction

1.1. As part of compliance with the PremiumTrust Bank information security policy, there may be circumstances where removable media will need to be used to store classified information. This document sets out how this should be done and what information should be recorded about the removable media and the user before it is issued.

1.2. The use of removable media such as USB memory sticks, CDs, DVDs, and storage cards to store PremiumTrust Bank data represents a significant risk to the PremiumTrust Bank and is strictly controlled under the information security policy.

1.3. Where removable media is currently being used in a business process, consideration must be given to the best method of achieving that business process by another means.

1.4. This document provides procedures concerning how requests for the use of removable media should be assessed and the appropriate recommendations that should be made depending upon the circumstances and requirements.

1.5. This control applies to all systems, people and processes that constitute the PremiumTrust Bank's information systems, including board members, directors, employees, suppliers and other third parties who have access to PremiumTrust Bank systems.

1.6. The following policies and procedures are relevant to this document:

- *Information Classification Procedure*
- *Information Labelling Procedure*
- *Asset Handling Procedure*
- *Backup Policy*
- *Teleworking Policy*

2. Selection of Removable Media

Where removable media of any format (CD, DVD, memory stick etc.) is used to store sensitive data, an assessment must be made of whether an alternative, more secure method can be used and if not, how best to secure the current method so that the risk to PremiumTrust Bank is minimised.

Such existing uses may include:

- Transfer of data to third parties e.g., suppliers, contractors, other agencies.
- Taking information home to work on.
- Backups of data in addition to scheduled server backups.

If an existing use is not in the above list but contravenes the information security policy, an alternative method of achieving the desired end result still needs to be identified.

The following tools are available from and supported by the IT Department:

- Remote access via a virtual private network.
- Encrypted memory stick.
- Secure file transfer.

The application of these tools to the identified requirements is considered below.

2.1. Data Transfer to Third Parties

2.1.1. Before considering alternative methods of data transfer, the following must be established:

- What data is being transferred?
- What is the business purpose of the transfer?
- Who is it being transferred to?
- What controls does the third party have in place to ensure the security of sensitive data?
- Is a confidentiality agreement required with the third party to provide assurance that our data will be protected?
- How often will the data be transferred, or is it a one-off event?

2.1.2. In most cases, the most secure method of data transfer will be via secure FTP which can be arranged by the Chief Technology Officer.

2.1.3. Only in exceptional circumstances where this is not possible an encrypted memory stick may be suitable, ideally taken to the third party by an

PremiumTrust Bank employee. Failing this, it should be sent by registered courier with a tracking facility and requiring a signature at the other end.

2.2 Taking Data Home to work on

2.2.1. In those cases where users are saving data to memory stick, CD or other removable media in order to take it home to work on using their own computer, it should first be checked that they are authorised to do this by their manager.

2.2.2. If they are, remote access using the virtual private network should be provided, in which case they are permitted to use their own PC. In the event that the user has no (or inadequate) Internet connection, an encrypted memory stick should be provided with a loan laptop (or a permanently assigned one if authorised for regular use).

2.3 Data Backups

2.3.1. Where users are taking their own backups of data onto removable media, they should be advised that this contravenes the information security policy and should refrain from doing so.

2.3.2. If there is a legitimate business requirement, arrangements may be made to perform an additional backup of key data to an additional server which remains on PremiumTrust Bank premises.

2.4 Taking Data Offsite

2.4.1. For those occasions where users need to take data to a third party site, perhaps to do a presentation or because they need to work at a contractors site for a few days, an appropriate tool should be selected based on the circumstances.

2.4.2. If internet access is available from the site they are working on, remote access via the virtual private network may be provided. Where such access is not available an encrypted memory stick should be provided.

3. Removable Media Issue Procedure

The following procedure should be used in those circumstances where removable media is requested for legitimate business purposes.

3.1 User Request is Received

3.1.1. The request for removable media should be received by the Chief Technology Officer via one of the standard methods (email, slack). The requesting user will then be asked to complete a form detailing the business reason for requesting removable media and, upon receipt, the request will be logged with the IT department with the completed form attached.

3.1.2. The Chief Technology Officer will then determine whether the use of removable media is the most appropriate method of achieving the business purpose that the user has. If the request for removable media is approved, then the rest of this procedure should be followed.

3.2 Order New or Allocate Existing Removable Media

3.2.1. If there are any new or re-usable removable media in stock these should be used instead of ordering new ones. Re-used removable media must be wiped of any existing data.

-

3.2.2. There is a password-protected spreadsheet that holds the following information about issued removable media:

- Asset Number
- Serial Number
- Password
- Allocated User
- Date of issue

3.2.3. Open this spreadsheet and create a new line for new removable media or find the correct line for re-issued removable media.

3.3 Set Removable Media Password

If appropriate to the type of removable media allocated, a password should be set. This must be at least 8 characters, have at least one capital letter, a

symbol and include a number. See the user manual for details on how to do this.

3.4 Record Information in Spreadsheet

Add the name of the allocated user to the spreadsheet and the date the removable media was issued. Ensure the following information is also recorded:

- Asset number
- Serial number
- Password
- Date of Issue

3.5 Inform User of Key Facts

3.5.1. Email the user that has requested the removable media. If several have been requested each person must be individually contacted.

3.5.2. Make them aware that:

- The removable media is fully encrypted – ALL data on it will be encrypted.
- The data will not be accessible without the password.
- If the password is lost, the data will NOT be recoverable.
- Do not write the password down or keep it with the removable media.
- You are advised not to change the password because if you do the Chief Technology Officer will not be able to help you if you forget it.
- The Chief Technology Officer must be informed if the removable media is lost.

3.5.2. Email confirmation that they have read and understood the above must be obtained before the removable media is sent out. The confirmation email should be saved on PremiumTrust Bank's shared drive.

3.6 Send Removable Media to User

The removable media should be taken or sent to the user by internal post or delivered by hand. The password must not be included.

3.7 Provide User with Password in a Secure Way

The password should be provided to the user by phone once they have received the removable media and their identity has been verified.

4. Disposal of Media

4.1 Requesting Secure Disposal

4.1.1. Requests to securely dispose of media should be logged with the Chief Technology Officer via email or slack. It is the responsibility of the owner of the media to inform the Chief Technology Officer of the need to dispose of the media.

4.1.2. The following details should be provided:

- Requester name, role, department and contact details.
- The type of media to be disposed of.
- The serial number of the media and/or device containing the media (e.g. PC), if available.
- The classification of the information held on the media if known.
- The location of the media.
- The reason for the media needing to be disposed of.
- When the media will be available for collection.

4.1.3. Note that it is the responsibility of the owner of the device or media to ensure that any required backups have been made of the data prior to requesting disposal. Once collected from site by the Chief Technology Officer data cannot be recovered.

4.2 Media Collection and Transport

4.2.1. The Chief Technology Officer will then arrange for the media to be collected via a secure means appropriate to the classification of the information held on it. In the meantime, the media should be protected appropriately prior to collection.

4.2.2. It may be appropriate to delay collection until a bulk pickup can be organised e.g. in the case of an office closure where many PCs are to be disposed of. Delayed collection should only be scheduled where the media can continue to be securely stored.

4.3 Confirm Details Provided

4.3.1. Once received from the requester the details of the media should be checked against those provided to verify accuracy and completeness. For

multiple disposals, an inventory of kit should be compiled with the following details:

- Device manufacturer, make and model
- Serial number
- Source
- Date of receipt

4.3.2. For individual requests this information may be stored on the shared drive raised at the time of the disposal request. The hardware asset register should be updated to reflect the fact that the device is no longer in live use and is pending disposal. Whilst awaiting disposal the equipment must be stored securely to prevent unauthorised access.

4.4 Choose Disposal Method

According to the type of media and the contractual arrangements in place with third parties, the Chief Technology Officer will then decide how best to dispose of the media.

4.4.1 Local Disposal

4.4.1.1. Where available, local facilities will be used to securely dispose of certain types of media. Media that may be locally disposed of may include:

- USB memory sticks
- Hard disks
- CDs and DVDs
- Solid state storage devices
- Floppy disks
- Phones and tablets

4.4.1.2. Only approved equipment e.g. a disk shredder may be used for local disposal.

4.4.2 Using a Third Party

4.4.2.1. For devices and media that require specialist equipment to securely destroy them a third party may be used.

4.4.2.2. The Chief Technology Officer should contact the third party to arrange a date and time for collection. Collection from site may also be an option to avoid the need to transport the kit more than necessary. The inventory of

equipment being collected should be checked and confirmed before leaving site so that all records are correct and up to date.

4.5 Disposal

4.5.1. The devices or media will then be disposed of using the chosen method. For local disposal, destruction should be witnessed by more than one person and the names of the people involved recorded.

4.5.2. For secure disposal using a third party the contractor will issue a certificate of disposal that complies with applicable legislation. The Chief Technology Officer will keep a record of these certificates.

4.5.3. Where appropriate, some of the equipment (or components of it) may be recycled in accordance with applicable legislation.

4.6 Record Disposal and Close Request

4.6.1. Once successfully disposed of the request record should be updated with the date, time and method of disposal and closed.

4.6.2. The hardware asset register should also be updated to reflect the fact that the equipment has been securely destroyed.