



Data Privacy Policy
Based on ISO/IEC 27001:2013
Version: 3.2

Corporate Information Security Guidelines

Preface

The Cogent E Services Private Limited (hereafter referred to as "Cogent") Information Security Management System (ISMS) Team assumes responsibility for this document and updates it as required to meet the needs of users. The Cogent ISMS Team welcomes and solicits feedback from users of this document and its reference artifacts so that future revisions of this document will reflect improvements, based on new technology, organizational best practices, and lessons learned. It will be maintained by the Information Security Manager (ISM) and is subjected to review at a minimum on a yearly basis.

Document Revision History

Version	Prepared by		Reviewed by		Approved by		Implementation Date	Summary of Changes
	By	Date	By	Date	By	Date		
0.1	ISM	03rd Dec'14	CISO	05th Dec'14	ISSC	-----	-----	Initial Draft
1	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	First Revision
1.0	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	New Template and updated document
1.1	ISM	13th Nov'15	CISO	13th Nov'15	ISSC	13th Nov'15	2nd Jan'16	
1.2	ISM	15th Oct'16	CISO	15th Oct'16	ISSC	15th Oct'16	31st Dec'16	
2.0	ISM	15th dec'17	CISO	15th dec'17	ISSC	15th dec'17	1st Jan'18	
2.1	ISM	22nd dec'18	CISO	22nd dec'18	ISSC	22nd dec'18	3rd Jan'19	
3.0	ISM	07 th Dec'19	CISO	07 th Dec'19	ISSC	07 th Dec'19	10th Dec'19	
3.1	ISM	07 Jul'21	CISO	07 Jul'21	ISSC	07 Jul'21	11th Jul'21	
3.2	ISM	07 Apr'22	CISO	07 Apr'22	ISSC	07 Apr'22	11th Apr'22	

Copyright

This document contains proprietary information for Cogent. It may not be copied, transferred, shared in any form by any agency or personnel except for authorized internal distribution by Cogent, unless expressly authorized by Cogent Information Security Steering Committee in writing.

Document Distribution

The Cogent Chief Information Security Officer (CISO) shall distribute this document to members of Information Security Steering Committee (hereafter referred to as ISSC) and Information Security Implementation Committee (hereafter referred to as ISIC).

The softcopy of the manual and related documents will be accessible to all employees in read-only mode through intranet server at location <http://172.19.197.214/Policies>

The CISO will ensure that any update to the Cogent ISMS is incorporated on the intranet server and is communicated to all employees of Cogent through an appropriate mode such as e-mail.

Distribution List

Name	Acronym
Information Security Steering Committee	ISSC
Information Security Implementation Committee	ISIC
Chief Information Security Officer	CISO
All employees and relevant external parties.	-

Conventions

The statements containing the words 'shall' and 'required to' in the document are mandatory rules. Failure to observe these rules may be construed as non-compliance to the policy.

The statements containing the words 'should' and 'recommended' imply a desirable requirement. Failure

Policy Statement

Cogent E Services Pvt. Ltd. regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its functions, and to maintain Confidence between those with whom it deals.









Purpose

The purpose of this policy is to ensure that the staff and Partners of Cogent E Services are clear about the purpose and principles of Data Protection and to ensure that it has guidelines and procedures in place which are consistently followed.

Principles

This includes the obtaining, holding, using or disclosing of such information, and covers computerized records as well as manual filing systems and card indexes.



To do this Organization Name follows the eight Data Protection Principles outlined in the Data Protection, which are summarized below:

-  Personal data will be processed fairly and lawfully
-  Data will only be collected and used for specified purposes
-  Data will be adequate, relevant and not excessive
-  Data will be accurate and up to date
-  Data will not be held any longer than necessary
-  Data subject's rights will be respected
-  Data will be kept safe from unauthorized access, accidental loss or damage
-  Data will not be transferred to organization outside unless that data has equivalent levels of protection for personal data

All these principles are extracted from Data Protection Act 1988.

Procedures

The following procedures have been developed in order to ensure that Cogent E Services meets its responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by Cogent E Services falls into 2 broad categories:

-  Management Data
-  Internal Data Records

Access

Staff will be supplied with a copy of their personal data held by the organisation if a request is made. All confidential Data must be opened by the addressee only.

Storage

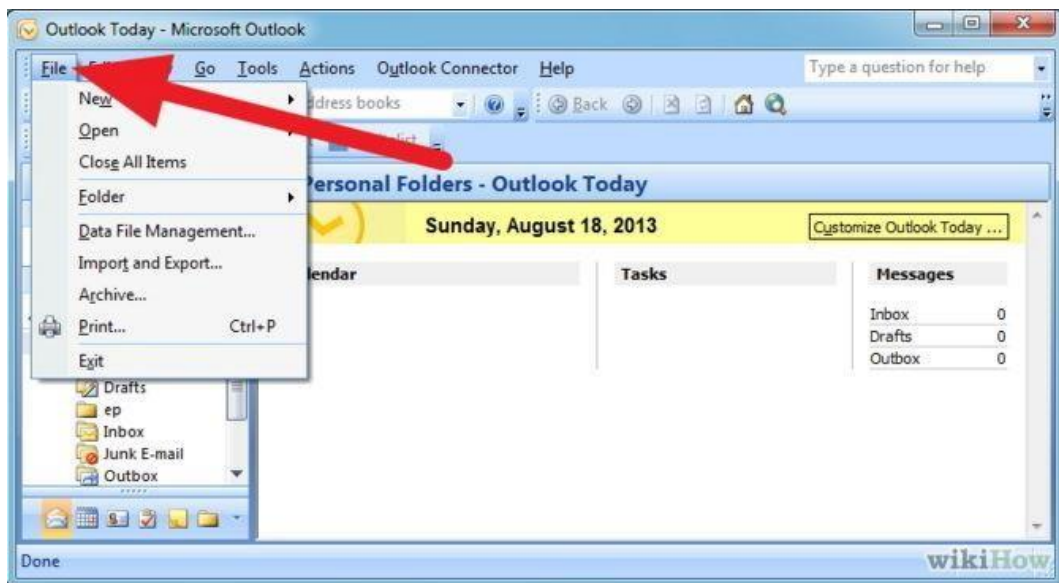
All data is kept in External Drive on File Server. Every effort is made to ensure data are stored in organised and secure systems.

Retention of Data

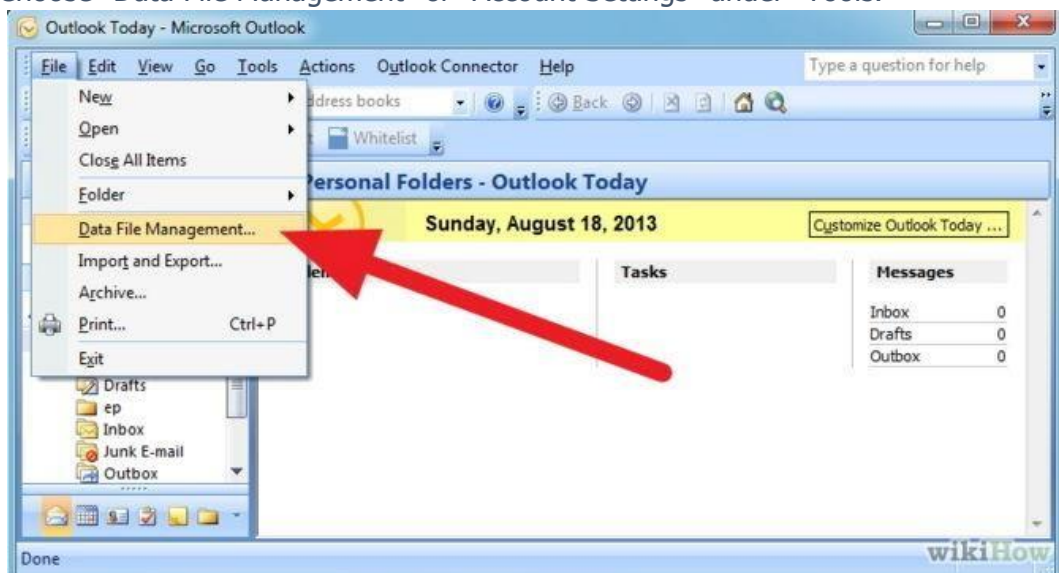
No documents will be stored for longer than is necessary. Information Technology associated data will be stored for 1 year.

Backup Microsoft Outlook Data

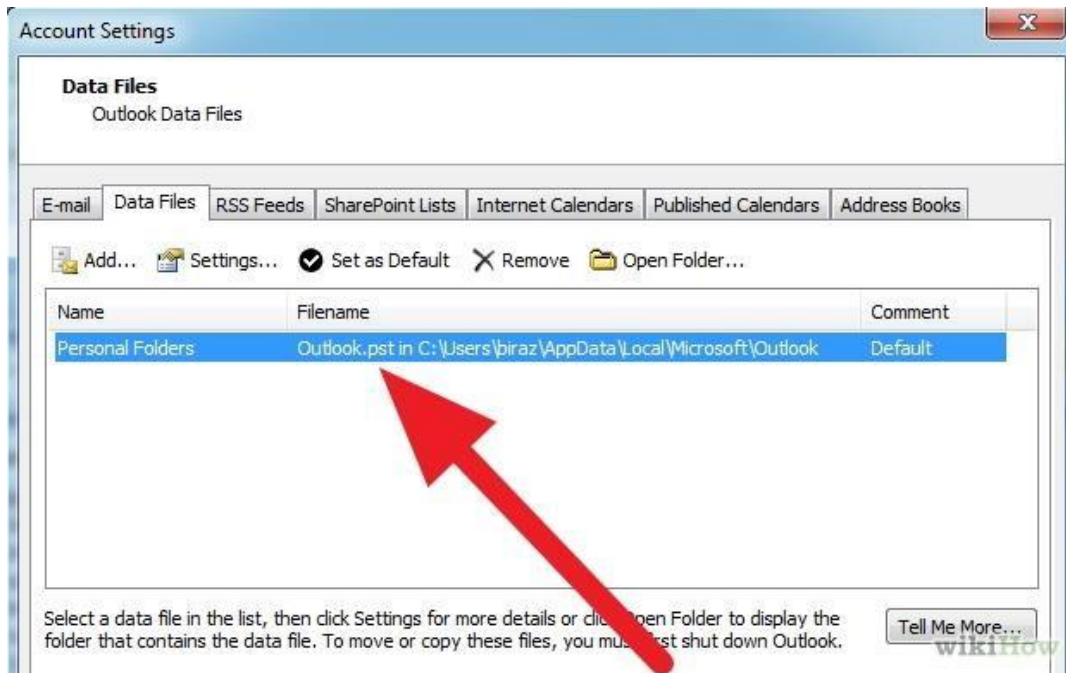
- 1) Look for Microsoft Outlook data in the Personal Folders file, which have a .pst extension. Outlook data includes messages, tasks, appointments, contacts and journal entries.
 - Select "File" from the top menu bar.



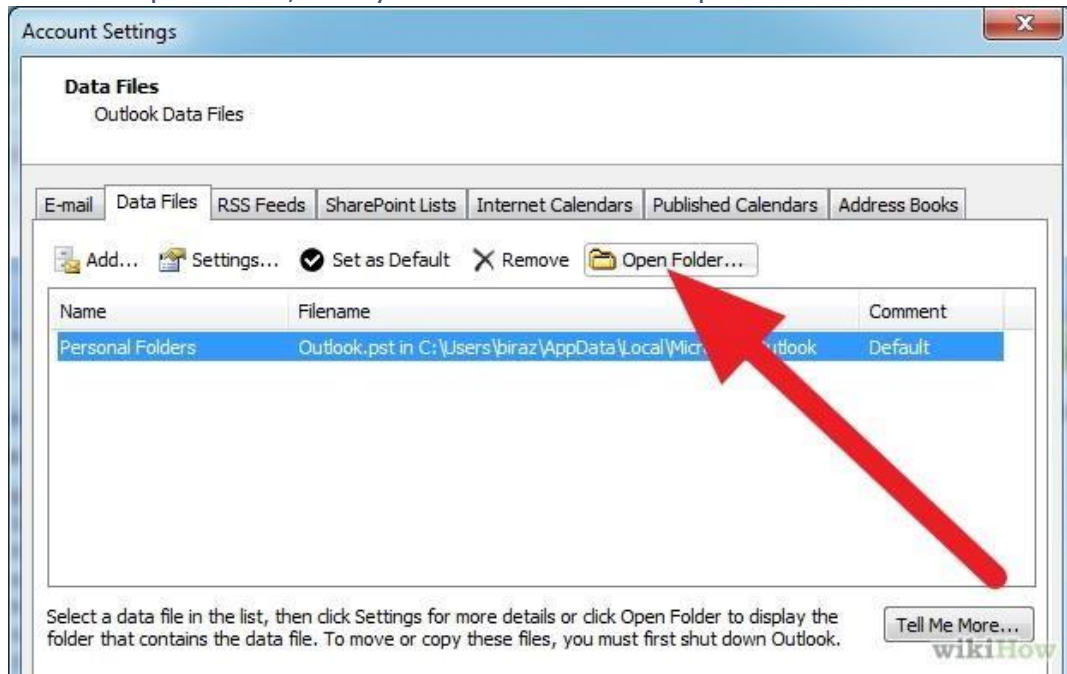
- Choose "Data File Management" or "Account Settings" under "Tools."



- Select the "Data Files" tab and highlight the files you want to back up.



- Click on "Open Folder," and you will be taken to the .pst files.



- Backup .pst files to removable media for protection or if you later need to restore files.
- Removable media includes USB flash drives and external hard drives.

