Exceedio IT Security Guide

Version 1.5 2016

Document Objectives:

To provide details on best practices for keeping Company computers, mobile devices and data safe when using email, the Internet, hardware, software and IT facilities.

To ensure effective IT security in daily operations

To understand the do's and don'ts of using computers and external devices

To promote awareness of common data cyber-attack methods and what we can do to protect the Company

IT Security Policy

	*1 Computer Use and Network Security*
	*2 Mobile and External Device Security*
	*3 Login and Password Security*
	*3.4 Email Security and Use*
	***3.5 Threat Prevention*** *(Malware and Virus Handling)*

Key

Symbol	Description	Symbol	Description
✓	*Do*	ⓘ	*For Your Information*
✗	*Don't*	👍	*Existing Actions*

IT SECURITY GUIDE

Computer Use and Network Security

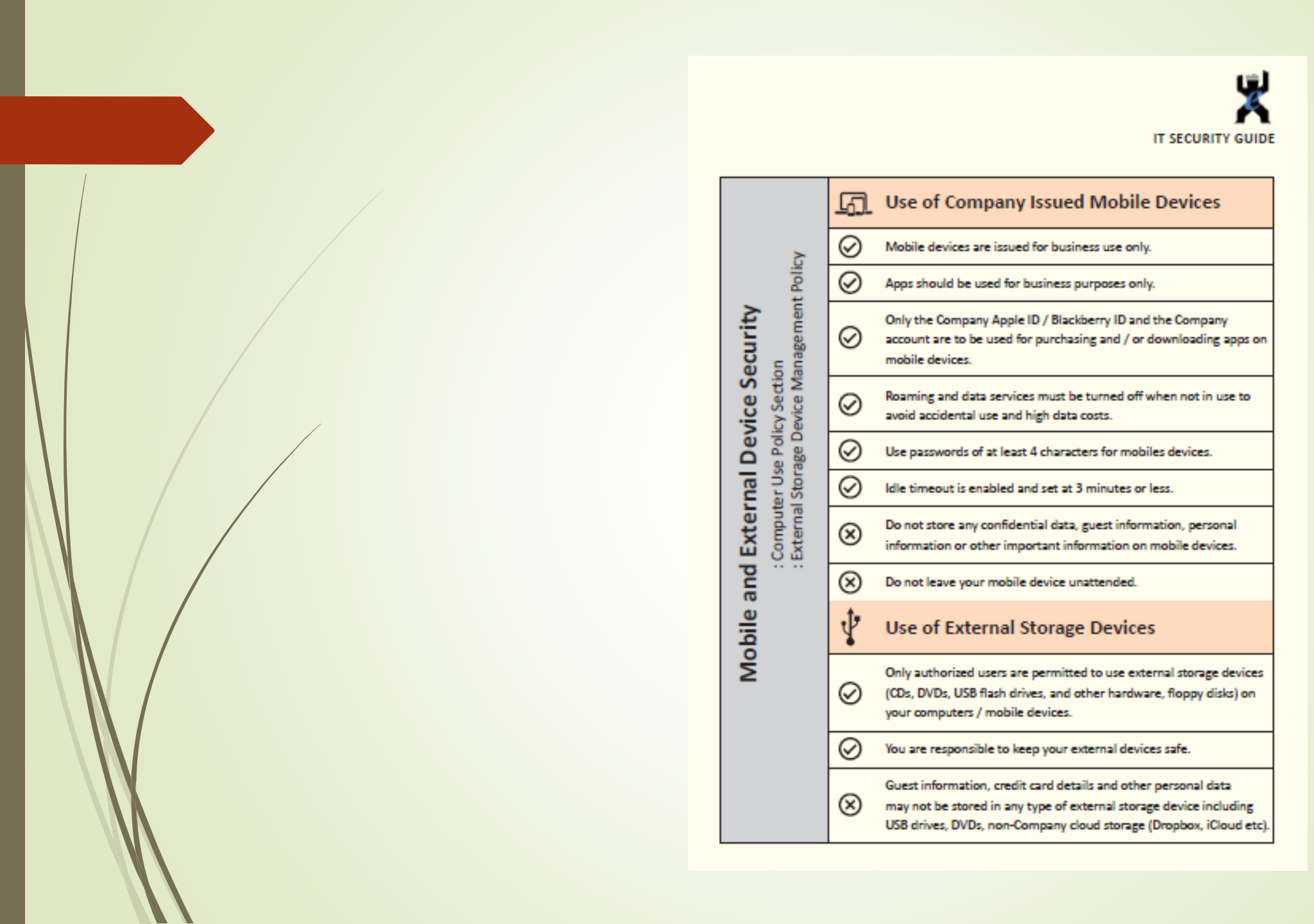
: Computer Use Policy
: Mobile Device Policy

Network Security

- ✓ Use the Internet and IT facilities for business-related activities only.
- ✓ Use trustworthy Wi-Fi sources only.
- ✓ Turn off your device's Wi-Fi connection when not in use.
- ✗ Do not disclose any proprietary information to anybody outside the Company.
- ✗ Do not click "Download" or "I accept" before reading instructions carefully.
- ✗ Do not allow external parties to access your computer or any network system without notifying Exceedio.
- ✗ In order to secure data and prevent any unauthorized access, do not save confidential data on shared resources accessible to others, for example, a network shared drive.
- ✗ Do not access or attempt to access any unauthorized information resources, IT system, databases, networks or other IT facilities.

Hardware and Software

- ✓ Hardware and software provided by the Company are to be used for business purposes only.
- ✓ Keep all confidential information which you are given access to secure and private at all times.
- ✓ Log off or lock your screen immediately when you are away from your computer or mobile device.
- ✓ Only use licensed and approved software provided by the Company.
- ✗ Do not download, install or upgrade any software without Exceedio review and approval.
- ✗ Personal notebooks or other personal electronic devices are not permitted for use with the Company network or IT facilities.


IT SECURITY GUIDE
Mobile and External Device Security
: Computer Use Policy Section
: External Storage Device Management Policy
Use of Company Issued Mobile Devices
Mobile devices are issued for business use only.
Apps should be used for business purposes only.
Only the Company Apple ID / Blackberry ID and the Company account are to be used for purchasing and / or downloading apps on mobile devices.
Roaming and data services must be turned off when not in use to avoid accidental use and high data costs.
Use passwords of at least 4 characters for mobiles devices.
Idle timeout is enabled and set at 3 minutes or less.
Do not store any confidential data, guest information, personal information or other important information on mobile devices.
Do not leave your mobile device unattended.
Use of External Storage Devices
Only authorized users are permitted to use external storage devices (CDs, DVDs, USB flash drives, and other hardware, floppy disks) on your computers / mobile devices.
You are responsible to keep your external devices safe.
Guest information, credit card details and other personal data may not be stored in any type of external storage device including USB drives, DVDs, non-Company cloud storage (Dropbox, iCloud etc).

IT SECURITY GUIDE

Login and Password Security

: Computer Use Policy Section
: Login and Password Policy

Keep Passwords Secure and Safe

- ✓ You must secure your own login IDs and passwords.
- ✓ Use at least 7-character passwords and include at least one alphabetic character and one numeral.
- ✓ Change your password at least every 180 days.
- ✓ Idle timeout for desktop and laptop computers is enabled and set at 30 minutes or less.
- ✓ Use password protection for sensitive information when transferring the information in a document.
- ✗ Do not share your login or password with anyone.
- ✗ Do not repeat the same password for any given account.
- ✗ Do not write down your password.

IT SECURITY GUIDE

Email Security and Use
: Email Policy

Use of Email Facilities
The Company's email system is to be used solely for business.
Check that recipients are correct before sending.
Company email transmissions to and from our email servers are encrypted.
Do not download attachments or click a link to download files without knowing what they are and the source.
Do not setup auto-forwarding of Company email to your personal email account.
Do not open or respond to email from unrecognized sources.
Do not reply to any phishing emails.
Enable spell checking and re-read your email before sending.
Do not write emails in ALL CAPITAL LETTERS.
Do not send racist, sexist or religion-specific material, offensive pictures or executable files intended to disrupt or offend the recipient.
Do not send chain letters, junk or spam email created or distributed via the Company email account.

IT SECURITY GUIDE

IT Threat Prevention
(Malware and Virus Handling)
: IT Threat Management Policy

Handling and Preventing Attack, Threat and Virus
✓ Keep the antivirus program activated all the times.
✓ Disconnect or switch off a virus-infected computer from the office network and contact the IT Department immediately.
✓ Run virus scans regularly.
✓ Be careful when downloading any files from the Internet that may be harmful to your computer.
✗ Do not ignore any warning messages on computers.
✗ Do not change antivirus program settings in your computer by yourself.
ⓘ On desktop and laptop computers, allow Windows operating system patch updates to complete before continuing work or shutting down.

Section 4:
Existing IT Security and Risk Management Activities

Network Security and Protection

Network Protection

- Firewall / Unified Threat Management (UTM) with the following key protections for the network:
  - ✓ DDOS protection (including network level)
  - ✓ Network firewall
  - ✓ Intrusion Prevention System
  - ✓ Http web proxy
  - ✓ Antivirus scanning for web proxy and SMTP email
  - ✓ Network malware detection including zero day attacks
- Antivirus programs must always be on at all workstations and on all servers.
- Patch deployment for all workstations and servers is scheduled on a regular basis.
- Remote access to the Company network is strictly controlled.
- Mobile Device Management (MDM) is in place for mobile devices.
- PCI compliance support for all credit card related applications is provided for all hotels and operations.

IT Policy and Procedures

- IT Policy and Procedures for all hotels and operations
  - ✓ To mitigate IT risks
  - ✓ To enhance the system protection and the controls in our network
  - ✓ To meet audit requirements
  - ✓ Accessible in Sphere
  - ✓ Continuously review and enhance with new technologies

New Vulnerability Alerts and Management

- Vulnerability management and communications
  (Monitoring and Prevention)
  - ✓ Monitor alerts from our sources to identify high risks items
  - ✓ Communication with the hotels and operations
  - ✓ Immediate action to mitigate risks
- Microsoft Monthly Security Bulletin Release Notifications

IT SECURITY GUIDE

Access Control Review and Network Assessment	**Users Permissions Review**	
	Main Line of Business Systems (LOB)	2 times a year
	Accounting Systems – e.g. Quickbooks	2 times a year
	On-Line Banking (Wells Fargo, Payroll, Asset Management)	1 time a year
	General Key Applications (e.g. Active Directory, Email)	1 time a year
	Vulnerability Assessment Scanning / Penetration Test	
	PCI ASV Vulnerability Scanning (Complete by PCI Approved Scanning Vendor) • PCI stands for Payment Card Industry • ASV stands for Approved Scanning Vendor	4 times a year

Future Security Protection (Late 2015-2016)

Data Monitoring and Encryption	**Personal Data Monitoring**	
	Active in Office 365 / Exchange Email Application	
	Monitor personal information, including credit card details and passwords.	
	Report issued for all emails with personal data.	
	Right Management Services	
	Users can set the permissions on Microsoft files for the specific internal staff to access or open files.	
	Integration with all Microsoft Office files such as Word, Excel PowerPoint, Outlook etc.	