# Policies & Procedures for Bring Your Own Device

## Background to this policy

Corporate IT departments face two challenges when contemplating a Bring Your Own Device (BYOD) policy: a mix of corporate and employee owned devices accessing the organization's network and data, and the use of those devices for both professional and personal purposes.

With data flowing across public networks, to and from devices that are easily lost or stolen, protecting data becomes a paramount concern and the primary driving force for implementing Mobile Device Management systems and policies. Security must be central to an organization's workforce mobility strategy in order to protect corporate data, maintain compliance, mitigate risk and ensure mobile security across all devices.

This outline policy gives a framework for securing mobile devices and should be linked to other policies which support your organization's posture on IT and data security.

As a Bring Your Own Device program can only be successfully implemented if certain security policies are enforced, we would expect a Mobile Device Management solution to be a prerequisite for this policy.

## Introduction

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and your organization supports their use to achieve business goals.

However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

Your organization has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

## Scope

All mobile devices, whether owned by your organization or owned by employees, inclusive of smartphones and tablet computers, that have access to corporate networks, data and systems are governed by this mobile device security policy. The scope of this policy does not include corporate IT-managed laptops.

Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.

Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

## The Policy Technical Requirements

1. Devices must use the following Operating Systems: (i.e. Android 7.0 and iOS 10 or later)
2. Devices must store all user-saved passwords in an encrypted password store.

3. Devices must be configured with a secure password that complies with your organization’s password policy. This password must not be the same as any other credentials used within the organization.
4. Only devices managed by IT will be allowed to connect directly to the internal corporate network. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

## User Requirements

1. Users may only load corporate data that is essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to your organization IT immediately.
3. If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with your organization’s incident handling process.
4. Devices must not be “jailbroken” or “rooted”* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact your organization IT.
7. Devices must be kept up to date with manufacturer or network provided patches. As a minimum patches should be checked for weekly and applied at least once a month.
8. Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
9. Devices must be encrypted in line with your organization’s compliance standards.
10. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify your organization IT immediately.
11. The above requirements will be checked regularly and should a device be non-compliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
12. The user is responsible for the backup of their personal data and the company will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
13. (If applicable to your organization) Users must not use corporate workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

*To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

## Actions which may result in a full or partial wipe of the device, or other interaction by IT:

1. A device is jailbroken/rooted.
2. A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user).
3. A device is lost or stolen.
4. A user has exceeded the maximum number of failed password attempt.

## Use of particular applications which have access to corporate data:

1. Cloud storage solutions: your organization supports the use of the following cloud storage solutions xxxxxx (i.e. Dropbox).
2. The use of solutions other than the above will lead to a compliance breach and the loss of access to the corporate network for the use.

While Intact Public Entities Inc. does its best to provide useful general information and guidance on matters of interest to its clients, statutes, regulations and the common law continually change and evolve, vary from jurisdiction to jurisdiction, and are subject to differing interpretations and opinions. The information provided by Intact Public Entities Inc. is not intended to replace legal or other professional advice or services. The information provided by Intact Public Entities Inc. herein is provided “as is” and without any warranty, either express or implied, as to its fitness, quality, accuracy, applicability or timeliness. Before taking any action, consult an appropriate professional and satisfy yourself about the fitness, accuracy, applicability or timeliness of any information or opinions contained herein. Intact Public Entities Inc. assumes no liability whatsoever for any errors or omissions associated with the information provided herein and furthermore assumes no liability for any decision or action taken in reliance on the information contained in these materials or for any damages, losses, costs or expenses in a way connected to it. Intact Public Entities Inc. is operated by a wholly owned subsidiary of Intact Financial Corporation. Intact Design® and Risk Management Centre of Excellence® are registered trademark of Intact Financial Corporation or its affiliates. All other trademarks are properties of their respective owners.