Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of MacDonald-Miller’s direct control. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers.
- Ultra-mobile PCs (UMPC).
- Mobile/cellular phones.
- Smartphones.
- PDAs
- Home or personal computers used to access corporate resources.
- Any mobile device capable of storing corporate data and connecting to an unmanaged network.

The policy applies to any hardware and related software that could be used to access corporate resources, even if said equipment is not corporately sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential client and business data that resides within MacDonald-Miller’s technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the company's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of MacDonald-Miller’s direct control to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Applicability

This policy applies to all MacDonald-Miller employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned mobile device to access, store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust MacDonald-Miller has built with its clients, supply chain partners and other constituents. Consequently, employment at MacDonald-Miller does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.
It addresses a range of threats to – or related to the use of – enterprise data:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss</td>
<td>Devices used to transfer or transport work files could be lost or stolen.</td>
</tr>
<tr>
<td>Theft</td>
<td>Sensitive corporate data is deliberately stolen and sold by an employee.</td>
</tr>
<tr>
<td>Copyright</td>
<td>Software copied onto a mobile device could violate licensing.</td>
</tr>
<tr>
<td>Malware</td>
<td>Viruses, Trojans, Worms, Spyware and other threats could be introduced via a</td>
</tr>
<tr>
<td></td>
<td>mobile device.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Loss or theft of financial and/or personal and confidential data could expose</td>
</tr>
<tr>
<td></td>
<td>the enterprise to the risk of non-compliance with various identity theft and</td>
</tr>
<tr>
<td></td>
<td>privacy laws.</td>
</tr>
</tbody>
</table>

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is supplementary to any previously implemented policies.

Responsibilities

The Chief Information Officer for MacDonald-Miller has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

All other staff shall adhere to the Technology Usage Policy for end-user responsibilities.

All MacDonald-Miller employees are responsible to act in accordance with company policies and procedures.

Affected Technology

Connectivity of all mobile devices will be centrally managed by MacDonald-Miller’s IT department and will utilize authentication and strong communication encryption measures. Although IT is not able to directly manage external devices – such as home PCs – which may require connectivity to the corporate network, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company’s infrastructure.

Policy and Appropriate Use

It is the responsibility of any employee of MacDonald-Miller who uses a mobile device to access corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct MacDonald-Miller business be utilized appropriately, responsibly,
and ethically. Failure to do so will result in immediate suspension of that user’s account. Based on this, the following rules must be observed:

**Access Control**

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the company’s systems, data, users, and clients at risk.

2. Prior to initial use on the corporate network or related infrastructure, **all mobile devices must be registered with IT**. MacDonald-Miller will maintain a list of required criteria for baseline functionality a mobile device will need to be capable of in order to be connected to the corporate infrastructure. Devices that do not conform to the listed criteria may not be connected to corporate infrastructure. If your preferred device does not possess all baseline criteria on this list, contact the Service Desk at Help@macmiller.com or 206-763-4357. Although IT currently allows only certain devices with specific criteria to be connected to enterprise infrastructure, it reserves the right to update this list at any time without notice.

3. All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by MacDonald-Miller’s IT department. Devices that have not been previously approved by IT, are not in compliance with IT’s security policies, or represent any threat to the corporate network or data will not be allowed to connect. Personal laptop computers or personal PCs may only access the corporate network and data via a Citrix connection using a cellular data internet connection, and unmanaged DSL/Cable internet connection, or the company provided “Guest Wireless” internet connection. Smart mobile devices such as smartphones, PDAs, and UMPCs will access the corporate network and data using Citrix and/or Exchange ActiveSync over the same data connections listed above.

4. An employee who travels to another country with a Mobile device which utilizes the company’s cellular communications account must request out-of-country data access (Data Roaming, International Cellular Service, etc.) in advance. This request must be approved by the employee’s supervisor. All out-of-country communication expenses incurred by the employee will be charged to the employee’s home department.

**Security**

5. **Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures.** All mobile devices must be protected by a **password**. The password strength will be determined and set by IT based in part on the employee’s software applications and device access to corporate resources. See the MacDonald-Miller’s password policy for additional background. **Employees agree to never disclose their passwords to anyone,** particularly to family members if business work is conducted from home.

6. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain or can provide access to enterprise data.
7. Passwords and other confidential data as defined by MacDonald-Miller’s IT department are not to be stored unencrypted on mobile devices. The user shall not attach a printed copy of the password to the device.

8. Any mobile device that is being used to store MacDonald-Miller data must adhere to the authentication requirements of MacDonald-Miller’s IT department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by MacDonald-Miller’s IT department before any enterprise data-carrying device can be connected to it.

9. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to breach or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with MacDonald-Miller’s overarching security policy.

10. Employees, contractors, and temporary staff will submit their device to IT for data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. Failure to submit the device to IT may result in the device being “remotely wiped” by the IT Department which will erase all data from the device, resetting it back to its factory default configuration.

11. In the event of a lost or stolen mobile device it is incumbent on the user to report this to IT immediately. IT will immediately change the user’s network password. If IT determines that the lost device presents a risk to the company, the device will be remotely wiped of all data. If the device is recovered, it can be submitted to IT for re-provisioning. This policy applies to all mobile devices.

12. MacDonald-Miller will allow an employee to bring in their personal number into one of the companies cellular vendors account at the discretion of the Telecommunications Manager. The end user’s line of service must not be under a contract as MM will add the line into our plan and will be assigned a company issued standard mobile smart phone and the line of service will now belong to MacDonald-Miller

13. In the event of termination or leave of the company, MacDonald-Miller will allow the end user to keep the line of service ONLY if the employee chooses to start personal services on the same cellular provider as what the line is on. MacDonald will not allow the end user to keep the hardware, it will be the end users responsibility to provide or purchase their own cellular device.

Help & Support

14. MacDonald-Miller’s IT department will support its sanctioned hardware, software, and data services, but is not responsible for conflicts, problems or loss of personal data caused by the use of unsanctioned media, hardware, software, or data services. This applies even to devices already known to the IT department. Unsanctioned categories include, but are not limited to:
   a. 3rd-Party mobile device “apps” other than Exchange ActiveSync
   b. Cellular Voice/Data services outside of MacDonald-Miller corporate accounts
   c. Mobile Devices, Laptops, PC’s or UMPC’s not purchased by official MacDonald-Miller IT Department procedures.

15. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of
MacDonald-Miller Facility Solutions

Mobile Device Acceptable Use Policy

MacDonald-Miller’s IT department. This includes, but is not limited to, any reconfiguration of the mobile device such as “Jail-breaking”.

16. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

Organizational Protocol

17. IT can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to MacDonald-Miller’s networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains MacDonald-Miller’s highest priority.

18. The end user agrees to immediately report to his/her manager and MacDonald-Miller’s IT department any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, passwords, etc.

19. Every mobile device user will be entitled to a training session around this policy. While a mobile device user will not be granted access to corporate resources using a mobile device without accepting the terms and conditions of this policy, employees are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

20. Any questions relating to this policy should be directed to Chief Information Officer

Policy Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

The (i) Chief Information Officer, and (iii) immediate Manager or Supervisor will be advised of breaches of this policy and will be responsible for appropriate remedial action which may include disciplinary action, including suspension or termination of employment.
Employee Declaration

I, ________________________________, have read and understand the above Mobile Device Acceptable Use Policy, and consent to adhere to the rules outlined therein.

_____________________________________  ____________  _____________
Employee Signature                Emp#                        Date