DALHOUSIE UNIVERSITY
Inspiring Minds

Information Technology Policy

5.3.3 Mobile Devices

Policy

Area: 5.3 Networks	**Date Issued:** 2010 Dec 01	
Title: 5.3.3 Mobile Devices	**Last Revision Date:** 2012 Jun 08	**Digitally Signed:**
Issued by: Telecommunications Manager, ITS	**Approved by:** Asst. Vice President – CIO, Dwight Fischer	

Purpose

This policy covers the provision and use of mobile devices. It is intended to contain costs and risks by establishing eligibility requirements and by setting standards for usage and configuration.

Policy Statement

Device Eligibility
Mobile devices and services will be provided for employees who meet the following criteria:

- Their defined role supports mission-critical services and is required to be reachable immediately; or
- Not usually at a fixed workstation and provides support where rapid response is often required; or
- Is in a role requiring frequent travel, mobile connectivity and rapid availability; or
- Demonstrates a need to have mobile access to critical information and documents

Device and Plan Selection
The standard plan includes voice services. Data and text plans are available. All plans require departmental approval.

ITS will work with the established vendor to provide a list of standard products and services that are supported by the University. If an employee desires a mobile device and plan separate from the standard options it is incumbent on the employee to arrange for service and support.

Usage
Mobile devices must be used and configured as detailed in the Procedures and Standards.

Management
ITS will select and operate the university's Mobile Device Management system to manage mobile devices accessing university academic and administrative systems. Circumventing the Mobile Device policy may result in being blocked from the university systems.

The Assistant VP / CIO Information Technology Services has the ultimate authority interpreting and administering the Mobile Devices Policy and associated Procedures and Standards.

Applicability of this Policy

The Mobile Device Policy and associated Procedures and Standards apply to all mobile devices. It applies to employees or other authorized representatives who are responsible for any mobile device issued by the University or conduct business on behalf of the University.

Procedures

Ordering a Mobile Device

An employee requiring the use of a University-owned mobile device must make an application to the appropriate Department Authority. Departments shall submit these requests directly to ITS or via the on line ordering tool. The request must contain the department name, device and plan selection, user hardware billing account information (if applicable) and monthly billing instructions.

Appropriate Use

1. Loss, damage or theft of a mobile device needs be reported as soon as reasonably possible to the ITS Telecommunications unit. Cost to replace a mobile device is determined by contractual agreements. The department authority may authorize the replacement of a mobile device. Department authorities may discontinue mobile device services at any time. Termination fees may exist and will be the responsibility of the department.
2. Employees must use discretion and abide by university privacy regulations pertaining to sensitive information as transmissions may not be secure.
3. Department authorities can ask to inspect the mobile device or review the billing charges at any time.
4. Employees are prohibited from using university-owned mobile devices for the purpose of illegal transactions, harassment, or obscene behaviour, in accordance with existing policy and government legislation.
5. Employees are expected to adhere to federal and provincial legislation governing the use of mobile devices.
6. Mobile devices are considered property of the University and are to be returned when no longer used for University business or the contract is fulfilled. A mobile device and associated account remain property of the department authority and may be reassigned or discontinued. When reclaiming mobile devices they must be cleared of data.
7. The University recognizes that mobile devices will incur incidental personal use. Any significant personal usage (including roaming, long-distance, airtime, data and text) that exceed the plan will be reimbursed to the university by the employee.
8. Any action that violates the manufacturer's warranty is not condoned on University-owned mobile devices.

Billing, Charges & Review

1. Plans will be established based on the need for employee use only. Standard services include call display, message centre and receiving text messages.
2. Mobile Devices may operate in wireless and/or mobile data mode. Use of University wireless networks is encouraged where possible to reduce operating costs.
3. Standard data plans are not designed for wireless laptop / tablet connections and can be very expensive. If tethering is required for University use on a mobile device an appropriate tethering plan is encouraged.
4. All costs associated with University-owned mobile devices will be charged to the appropriate department.
5. Monthly bills will be sent to the department for review and authorization of payment. Department authorities must review bills to identify irregular usage and ensure selected plans best suit business needs.

University business calls made on personal mobile devices that incur additional cost may be reimbursed when:

1. Department pre-approval is required.
2. Department authority will authorize reimbursement requests through cheque requisition.
3. A copy of the detailed bill must be submitted with the requisition. The bill should identify to whom calls were made or received from. Employees may be required to provide additional information that the University may reasonably request.

International Travel – Roaming

Usage outside Nova Scotia and Canada will result in additional charges and the fees may be substantial. Travel plans may be added prior to travelling, as required. ITS requires 3 business days notice to process the request.

Non-Compliance

The Assistant Vice President Information Technology Services, and an immediate Manager will be advised of any breach of this policy and be responsible for appropriate remedial action, which may include revocation of privilege to use University-owned mobile devices or disciplinary action

Standards

1. Data encryption is required on all mobile devices.
2. Employees will use good password practices.
3. Mobile devices will be set to erase after no more than 10 successive failed password attempts.
4. Mobile devices will be configured to lock after 15 minutes of inactivity.

Guidelines

1. Tagging mobile devices with contact information is recommended as an aid to recovery after loss or theft.
2. Dalhousie VPN is strongly encouraged whenever connections are made from non-Dalhousie networks

Definitions

mobile device

> Mobile device means all cellular phones, pagers, smartphones and, includes all wireless data devices (such as Tablets, USB wireless modems, etc.).

department authority

> Department authorities have spending authority within a unit.

Related Documents

Electronic Record Destruction Standards:	http://its.dal.ca/security/data_protection/#eDestruction
Data Classification Schema:	http://its.dal.ca/policies/data-classification.pdf
Personal Information Intl Disclosure Protection Act:	http://nslegislature.ca/legc/bills/60th_1st/3rd_read/b019.htm
Dal Alert service:	https://dalalert.dal.ca
Dalhousie VPN:	https://wireless.dal.ca/vpn/usingvpn.html

Revision History

2012 June 08	Edits for mobile device management
2011 October 26	Added link to Data Classification Schema
2011 September 29	Minor edits for clarity and emphasis
2011 September 01	Promoted from Provisional to Policy
2011 March 24	Minor Revisions
2010 December 01	Draft