

Policy

Area: 5.3 Networks	Date Issued: 2010 Dec 01	
Title: 5.3.3 Mobile Devices	Last Revision Date: 2011 Oct 26	Digitally Signed:
Issued by: Telecommunications Manager, ITS	Approved by: Assistant Vice-President/CIO, ITS	

Purpose

Mobile devices can be costly to the University in operating costs and in employee down-time when the devices fail to perform as expected. The devices can also expose the University to the risk of data loss or theft. This policy is intended to reduce mobile device costs and risks by establishing who is eligible for mobile devices, how the devices are to be used, and how the devices are to be configured.

Policy Statement

Mobile devices and plans will be provided based on job requirements but will only be provided when the employee:

- Supports mission-critical systems or provides critical campus services and is required to be reachable immediately both within and beyond normal business hours; or
- Is not normally present at a fixed workstation and provides nomadic support of which 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

A plan that maintains voice communications and ability to receive DAL Alert text messages is the standard. If an employee has a demonstrated need to have a texting and/or data plan or tablet plan, then approval of such plans will be at the discretion of the Department Authority.

The final decision on whether an employee will be issued a mobile device rests with the University Department Authorities. However, mobile devices will not be issued to student workers, contract employees, part-time, temporary personnel, consultants, or other workers that do not have a compelling use for the technology.

ITS will administer and negotiate mobile contracts on behalf of the University. ITS has standardized mobile devices, service packages, and accessories for use in the Dalhousie University environment. **Only those mobile devices approved by ITS will be authorized and supported.**

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

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 Policy and associated Procedures and Standards cover all wireless mobile devices such as cellular phones, smartphones, pagers, tablets and mobile data sticks and apply to all employees or other authorized representatives who have or are responsible for any mobile device issued by the University or conduct business on behalf of the University while using any mobile device.

Procedures

Ordering a Mobile Device

Employees requiring the use of a University-owned mobile device must document their need by applying to their Department Authority.

Email correspondence from a Department Authority to the ITS Telecommunications Manager / Unit will serve as authorization for an employee. The application request must contain department name, user hardware billing account information (if applicable) and monthly billing instructions.

The ITS Telecommunications Manager and staff are available to advise on the most effective plan and on device availability.

Appropriate Use

Only University employees and other authorized representatives of the University may use these devices and they must observe the following:

1. University-owned mobile devices are the property of Dalhousie University and must be treated, used, and safeguarded as such. Loss or theft of a device must be reported immediately to the Department Authority and the ITS Telecommunications Manager / Unit who will request service suspension. If an employee damages a university-issued mobile device, the employee must notify the Department Authority and ITS Telecommunications Manager immediately to assess risk. The cost to replace a lost, stolen or damaged device is determined by any existing contractual agreements (The ITS Telecommunications Manager and staff can provide current pricing information.) It is at the discretion of the Department Authority to authorize the replacement or upgrade the device.
2. Employees must use discretion in relaying confidential information on mobile devices as transmissions may not secure.
3. There should be no expectation of privacy as Department Authorities can ask to see the mobile device or review the charges on the bill.
4. No employee is to use a university-owned mobile device for the purpose of illegal transactions, harassment, or obscene behaviour, in accordance with other existing employee policies and government legislation.
5. Employees issued a mobile device with a camera and or video camera feature etc. shall not use this feature in a way that violates the University's Surveillance Policy or any provincial and federal laws governing the recording of audio, video, or photographic images.
6. Employees must adhere to provincial legislation governing the use of mobile devices while operating a vehicle.
7. In accordance with the Personal Information International Disclosure Protection Act (PIIDPA), transporting the devices outside of Canada need to be considered carefully. "The personal information held by public bodies and municipalities may be transported temporarily on, or accessed from the laptop computers, cell phones, and other electronic devices (e.g. blackberries), outside Canada if the head of the organization determines it is necessary to meet the operational requirements of the organization, or is necessary for the work of the employees." (Government of NS PIIDPA FAQ).

8. Department Authorities may deactivate a device and terminate related services at any time. However, termination fees may exist and will be the responsibility of the Department Authority. The ITS Telecommunications Manager and staff are available to identify those costs restrictions.
9. Discarded mobile devices are the property of the university department. Mobile devices shall be considered discarded if they are no longer used by the University and the individual's contract term is fulfilled.
10. Upon termination or resignation of an employee, the device and its associated service number remains the property of the Department Authority and may be reassigned or discontinued.
11. When discarding or reassigning mobile devices, the mobile devices must be cleared of data. (See Related Documents section for procedures for electronic data destruction).
12. Unless authorized, any enhanced services such as downloading songs or applications, texting, surfing the internet or any features that would incur additional monthly costs are not permitted
13. The University recognizes that cell phones will be used for incidental personal use. Any charges that exceed the plan that include significant personal usage (including roaming, long-distance, airtime, data and texting) will require the employee to reimburse the University through the Department Authority.
14. Neither 'Jailbreaking' nor any other action that violates the manufacturers warranty will be permitted on University provided devices.

Voice, Data and Texting Plans

To take advantage of volume pricing and discounts, ITS will negotiate contracted rates for voice, data and texting plans. The following will apply:

1. Plans will be established based on the need for employee use and will not consider personal use as a factor. Standard services will include call display, message centre and the ability to receive Dal Alert text messages.
2. **All mobile devices using data plans must run a data, voice and texting usage measuring application.** The purpose of this tool is to make the user aware of the cost of operating the device and to assist in selecting the appropriate data and texting plans. These applications are free and available from the smartphone manufacturer.
3. The ITS Telecommunications Manager / Unit is available to provide consulting and advisory services to assist in selecting optimal plans.
4. To activate a Smartphone (e.g. BlackBerry, iPhone, Android, Windows 7 & etc.) on the mobility network, it must carry an appropriate data plan and the ability to receive text messages.
5. Tablets operate in Wi-Fi and/or mobile data mode. If using a mobile data mode then a mobile data plan is required. The ITS Telecommunications Manager and staff are available to assist the department in selecting the appropriate mobile data package.
6. Wi-Fi is available in many regions of the University's three campuses. To reduce operating costs mobile devices must, wherever possible, be programmed to use the University's Wi-Fi network while it's in range.
7. Typically the initial set up of the smartphone / tablet requires a large volume of data. To help reduce the data costs associated with the initial set up; it is strongly recommended that the device be set to Wi-Fi mode for the initial setup and programming.
8. Tethering and laptop wireless services - Dalhousie's standard cellular plans are not designed for wireless laptop connections. If this service is required for university use then the cell user and Department Authority will work with the ITS Telecommunications Manager / Unit to determine the most cost effective tethering/laptop wireless plan.

International Travel – Roaming

Dalhousie's standard plans for voice, data and texting are designed for use only within Nova Scotia and within Canada. Usage outside these areas will result in additional charges and the fees may be substantial.

To reduce these travel costs, various voice, data and texting plans can be added when needed.

Prior to traveling, the mobile device users **must** contact the Department Authority and arrange to have the appropriate plan added. The ITS Telecommunications Manager / Unit will be available to assist the department in selecting travel packages.

Billing, Charges & Review

1. All costs associated with university-owned mobile devices will be allocated to the appropriate department.
2. Monthly itemized bills will be sent directly to the department and must be reviewed and authorized for payment by the Department Authority, with costs allocated to the appropriate cost center/account number. Department Authorities must review the bill to identify any irregular usage patterns and to ensure plans selected best suit the business needs.
3. The ITS Telecommunications Manager and staff are available to assist in selecting plans and billing review.

Reimbursement for Phone Calls

Employees may be reimbursed for University business calls made on their own Mobile devices however access charges or other monthly recurring charges are the responsibility of the employee and will not be paid by the University. In order to be reimbursed, the following conditions must be met:

1. Department pre-approval is required for reimbursement to be considered.
2. Reimbursement requests will be submitted to the Department Authority who will authorize the amounts through a cheque requisition. The rationale for the reimbursement is to include any or all of the criteria in Appropriate Use section (above).
3. No reimbursement will be made to employees for business calls made on their personal mobile phones if they do not incur additional direct costs.
4. A copy of the detailed phone bill must be attached to the requisition. If the service provider does not provide detailed billing, the employee must request that they do so in order to be reimbursed. If the copy of the bill does not list whom the calls were made to (or received from as the case may be), the employee will be required to provide any such further information as the University may reasonably request.

Policy Non-Compliance

The Vice-President Finance, Assistant Vice President ITS, and the employee's immediate Manager will be advised of any breaches of this policy and will be responsible for appropriate remedial action, which may include revocation of the privilege to use university-owned mobile devices and or disciplinary action.

Standards

1. Only devices which have provision for password protection will be issued by ITS and the following password-specific settings must be applied whenever the features exist:
 - 1.1. the password protection must be configured to automatically lock the device no more than 15 minutes after last use
 - 1.2. devices must be set to erase after no more than 10 successive failed password attempts
2. Passwords must be chosen such that guessing them will be difficult, even for someone knowing the user. Repetitively entering a long password into small devices is not convenient. Therefore passwords may be as short as four numeric characters but employees are encouraged to use longer passwords and/or passwords with a mix of numbers and letters where convenient.
3. Data encryption is highly desirable but may not be supported on all devices.
 - 3.1. Where encryption is available it must be enabled and set at the highest setting possible. The encryption must include all data on the device and on associated media cards (where the media cards hold any University data)
 - 3.2. Where encryption is not available, the device must not be used to store passwords or any other University data at a 'Sensitive' or higher classification.

4. Wi-Fi connections to any network other than Dalhousie's wireless network must use Dalhousie's VPN service. Devices not capable of connecting via Dalhousie's VPN must not be used on non-Dal Wi-Fi networks while transmitting passwords or any other Dalhousie data at a 'Sensitive' or higher classification.
5. All University provided devices must be marked, either electronically (as 'wallpaper') or by decal, with a contact name and phone number to aid in recovery. Either the University's official Lost and Found number (494-6400) or the user's department number must be indicated.
6. Malicious software (malware) is a growing problem on mobile devices. As and when anti-malware solutions become available ITS will begin installing them. Older devices may require retroactive installation. Users of the devices must not remove or disable the anti-malware software without authorization from ITS. must be included.

Guidelines

N/A

Definitions

Mobile device Mobile Device in this document means all cellular phones, pagers and smartphones (such as BlackBerry, iPhone, Android & Windows 7 devices) and also includes all wireless data devices (such as Tablets, USB wireless modems, Turbo Sticks, Turbo Hubs, etc.).

Department Authority Department Authorities are the individuals having spending authority within their unit.

Jailbreaking Jailbreaking is a process that allows users of certain devices to gain root access to the command line of the operating system thus removing any limitations imposed by the manufacturer.

Related Documents

Electronic Record Destruction Standards:

http://its.dal.ca/depts/security/data_protection/#eDestruction

Data Classification Schema:

<http://its.dal.ca/policies/data-classification.pdf>

Personal Information International Disclosure Protection Act:

http://nslegislature.ca/legc/bills/60th_1st/3rd_read/b019.htm

Dal Alert service: <https://dalalert.dal.ca>

Revision History

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