وزارة المواصـــلات والاتصـــالات
Ministry of Transport & Communications

Bring Your Own Device (BYOD) Security Policy

Ministry of Transport & Communication 'MOTC'

7th March 2016

Version: 1.0
Classification: Public

Document History

Version	Date	Comments	Author
1.0	05-01-2016	Final Document	CS Policy & Standards Section

Table of Contents

Definitions and Abbreviations:

- Agency: Government and / or Semi Government organization and / or Critical Sector Organization and / or organizations that are adopting this policy.
- BYOD: Bring your own device
- Device: Computing device that can store and / or process and / or transmit / receive information.
- Device environment: Both the device's hardware and software
- Controlled Network: Any information system (including end points such as desktops / laptops / servers etc) and / or network that comprises part of your corporate secure network.
- Requirement: A provision that the responsible party must agree to in order to be compliant with the policy
- Responsibility: A task, action or requirement that the responsible party must agree to be held accountable for in order to be compliant with the policy
- Private data: Data that is stored on a user's device and is irrelevant to the proceedings of an organization
- Tablet: An open-face wireless device with a touchscreen display and without physical keyboards. The primary use is the consumption of media; it also has messaging, scheduling, email, and Internet capabilities. Tablets may have open-source OSs (such as Android) or a closed OS under the control of the OS vendor and/or device make (such as Apple's iOS and Windows). Media tablets may or may not support an application store.
- Critical Sector Organization (CSO): Key Organizations within the critical sectors.

1. Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

This Policy Document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Policy Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

2. Introduction

With the rapid development in the growth, innovation and consumerization of technology, computers have become powerful and affordable.

This has posed an interesting dilemma to organizations globally. Whilst the use of technology empowers users and increases productivity (the user being able to work from anywhere and being online all the time), it has stretched the organizations in terms of not only providing infrastructure support to such technology but also being able to innovatively secure their information which is now being spilled over their physical boundaries. Add to this scenarios where employees would like to choose or use their own device.

This policy expects to set the tone and expectations within an agency to deal with the current scenario wherein users would like to use their own devices for official work (Bring Your Own Device (BYOD)) or have a say in the choice of devices being made available to them.

Device Ownership Models

Bring Your Own Device (BYOD): employees get full responsibility for choosing and supporting the device they use at work because they're bringing in their personal one. This method is popular with smaller companies or those with a temporary staff model.

Choose Your Own Device (CYOD): employees are offered a suite of choices that the company has approved for security, reliability, and durability. Devices work within the company IT environment, but the employees own their phone — either they paid for it themselves and can keep it forever, or the company provided a stipend and they can keep it for the duration of their employment.

Company-Owned, Personally-Enabled (COPE): employees are supplied a phone chosen and paid for by the company, but they can also use it for personal activities. The company can decide how much choice and freedom employees get. This is the closest model to the traditional method of device supply, Corporate-Owned Business Only (COBO).

3. Scope and Application

This policy is applicable to the following type of devices:

- ✓ Any Computing device that can store and / or process and / or transmit / receive information when connected to the controlled network[1].

The policy applies to all agencies , however its application is as follows:

Mandatory: Government Agencies

[1] Controlled Network: Any information system (including end points such as desktops / laptops / servers etc) and / or network that comprises part of your corporate secure network.

The Controlled Network primarily consists of three zones, De-Militarized zone where all servers are located, user zone where all user devices are located and public zone with very little or no control where public information or access is allowed.

The policy explicitly prohibits use of devices not owned and managed by the agency within the demilitarized zone.

The policy does not prohibhit the use neither controls the use of devices not owned and managed by the agency within the public zone.

The policy is explicitly applicable for devices that are not owned and managed by the agency being intended to be used in the user zone.

Recommended: Critical Sector Organization
Optional: Other Corporate Organizations

4. Policy Statements

4.1. Governance

The agency shall include security of BYOD within their information security programme to ensure risks are minimized when employees, contractors, consultants and/or general public (if applicable) connect uncontrolled[2] devices to agency ICT systems.

4.1.1. The agency shall conduct formal analysis for its need to allow or disallow BYOD devices within their environment, the analysis should at least be based on identifying the risks that it may introduce, effectiveness of existing security controls, cost benefit analysis and applicable legal and regulatory requirements[3].

4.1.2. The agency shall document, approve, publish, communicate, enforce and maintain its BYOD policy, the policy at minimum must include

- 4.1.2.1. Scope including
  - 4.1.2.1.1. All employees, contractors, consultants or general public (if applicable)
  - 4.1.2.1.2. All office locations including Head Office, Branch offices and/or any other production facility or work area
  - 4.1.2.1.3. All ICT networks including corporate network, Internal LAN, Internet Zone, Guest Network and/or DMZ
- 4.1.2.2. Agency decision of BYOD;
- 4.1.2.3. Privacy concerns;
- 4.1.2.4. responsibility for policy implementation;
- 4.1.2.5. Mandate to comply;
- 4.1.2.6. Security controls to protect agency data and systems;
- 4.1.2.7. Compliance review and;
- 4.1.2.8. Exception management.

4.1.3. The head of agency shall by accountable for BYOD security policy and shall ensure completion of implementation activities of security controls and compliance status are up-to-date. 4

4.1.4. The head of agency shall ensure continual improvement within their agency with

- 4.1.4.1. Appropriate and adequate training to its employees, contractors, consultants or general public (if applicable); at least annually
- 4.1.4.2. Conducting internal compliance assessment to ascertain effectiveness of controls; at least annually
- 4.1.4.3. Maintenance of policy as when agency environment, ways of working, applicable laws, regulations and/or policy changes are identified.

[2] Devices that are not supplied and/or managed by agency, these devices may not have adequate security controls, up-to-date security patches or anti virus and when connected to controlled network i.e. agency network may compromise confidentiality, integrity and/or availability of sensitive information or systems.

[3] In case of conflicting policies, laws and/or regulations, the laws of state of Qatar will prevail and most robust and strict control must be considered.

[4] The head of agency may choose to delegate responsibility for implementation but will always be accountable for enforcement and compliance of policy.

4.2. Security Controls

The agency shall ensure confidentiality, integrity and availability of its data and/or systems is not impacted in any way with introduction of BYOD and shall deploy reasonable security controls including, but not limited to

4.2.1. **Acceptable Usage** – The agency shall ensure

- 4.2.1.1. BYOD devices are allowed within the agency on need basis with valid business justification; documented and approved
- 4.2.1.2. BYOD devices used within the agency are compliant to laws and regulations within State of Qatar
- 4.2.1.3. BYOD devices utilize connection from licensed operators within State of Qatar
- 4.2.1.4. BYOD devices use legitimate (non pirated, hacked or jailbroken) software, operating system and/or connections.
- 4.2.1.5. The BYOD services are enabled upon acceptance of terms of service (usage of BYOD) including but not limited to user responsibility, security obligations, responsible usage, Data disposal (secure and / or remote wipe of data), NDA and privacy consent by the employees, contractors, consultants and/or general public (if applicable)

4.2.2. **Provisioning** – The agency shall ensure

- 4.2.2.1. Documented, approved and communicated process to request the BYOD service to employees, contractors, consultants and/or general public (if applicable)
- 4.2.2.2. The access management process includes formal management of grant, change and/or revoke of access rights, services and or applications.
- 4.2.2.3. The access to data, systems and/or application is provided on need to know basis following principle of least privilege.
- 4.2.2.4. Access permissions w.r.t. agency data, systems and/or services cannot exceed user entitlement based on agency network security, data access, data classification policy
- 4.2.2.5. Applications from untrusted sources and/or third party stores should be controlled and allowed only after analysis and explicit approval.
- 4.2.2.6. Maintenance of records of approvals for access and/or acceptance of terms and an inventory of all devices connecting to secure / enterprise network / device with necessary details.
- 4.2.2.7. Accountability of user action when/if multiple users are using same BYOD device[5]

4.2.3. **Management** – The agency shall ensure

- 4.2.3.1. Password based access control on all BYOD devices compliant to agency password policy and National Information Assurance (NIA) policy where applicable.
- 4.2.3.2. Enabling of time out automatic locking of BYOD device when not being used for 5 minutes where applicable.
- 4.2.3.3. The users of BYOD device cannot extend or connect to non secure or untrusted networks using wireless, radio, Bluetooth, usb modems etc while connected to secure enterprise networks and / or devices.
- 4.2.3.4. Agency sensitive data cannot be copied to and/or accessed by uncontrolled device connecting to BYOD device[6]

[5] This may be achieved by provisioning multiple profiles with access control wherever possible.
[6] Example – Agency employee should not be able to copy or access agency confidential data by connecting his personal laptop to BYOD device using USB, WiFi, Bluetooth and/or any other connection

4.2.4.**De-provisioning** – The agency shall ensure

4.2.4.1. Mechanism/process to cancel the service and/or access for BYOD device.

4.2.4.2. Service and/or access is cancelled when employees, contractors, consultants and/or general public (if applicable) is no longer required to work for department, agency or specific job function.

4.2.5.**Disposa**l – The agency shall ensure

4.2.5.1. Agency data, credentials, certificates and applications are securely removed from BYOD device when user is no longer working for the agency or changes in this work profile or as when access control policies changes or when device is reported missing or stolen or replaced.

4.2.5.2. Access logs are secured as per retention policy and/or at least 6 months and are securely disposed once they are no longer needed as per compliance to policy, regulation and/or law

4.2.6.**Privacy** – The agency shall ensure

4.2.6.1. Compliance to privacy laws, regulations, policies and/or practice while enabling, managing and disabling BYOD devices

4.2.6.2. The user is made aware of sensitive data being fetched, processed, extracted and/or researched when they subscribe to BYOD services

4.2.6.3. The user understands and approves, explicit consent on sensitive data being transmitted, processed and/or stored by agency systems for BYOD services

4.2.6.4. Security of user sensitive data transmitted, processed and stored through the BYOD process

4.2.7.**Cloud7** - The agency shall ensure

4.2.7.1. The employees, contractors, consultants and/or general public (if applicable) using BYOD is not violating the government cloud security policy, applicable laws and regulations related to transmission, processing and/or storage of data outside State of Qatar.

4.2.7.2. Effectiveness of reasonable security controls to restrict storage, processing and/or transmission of classified data as per policy, regulation and/or law

4.2.8.**Encryption** – The agency shall ensure

4.2.8.1. Agency data being transmitted and/or stored8 on or using BYOD devices is encrypted using strong encryption algorithm.

4.2.8.2. Effective key, certificate and/or passphrase management process is established.

4.2.9.**Physical** – The agency shall ensure

4.2.9.1. Reasonable9 physical security measures are enforced, maintained and reviewed within restricted areas like data center, user work areas etc. to avoid introduction of rogue or unauthorized BYOD devices

4.2.10. **Audit Logging** – The agency shall ensure

---

or storage mechanism; Endpoint security or data leakage prevention or similar technologies may be utilized

[7] Example - Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by an international hosting company.

[8] Stored on device inbuilt storage or extendable storage in the form of media cards, USB, cloud storage etc.

[9] Physical security controls may include but not limited to manned security guards, video surveillance, frisking, access control doors etc.

4.2.10.1. All events including, but not limited to system, security, authentication, application, data or system access etc. are logged, secured and stored at a central repository within the agency owned information systems

4.2.10.2. The audit logs are reviewed regularly to identify any anomaly or breach to policy; at least monthly

4.2.10.3. The audit logs are retained for at least 6 months and/or as per agency data retention policy based on applicable laws and regulations within State of Qatar.

4.2.11. **Incident Management** – The agency shall ensure

4.2.11.1. Incident reporting and handling process within the agency are updated to address incidents related to BYOD devices including but not limited to lost, stolen, unauthorized access, breach of policy etc.

4.2.11.2. All employees, contractors, consultants and/or general public (if applicable) are aware of incident reporting procedure related to BYOD devices being used to transmit, process and/or store agency data.

4.2.11.3. Severe incidents are reported to Q-CERT, regulator and/or applicable law enforcement agency as soon as incidents are confirmed.

4.2.12. **High Risk Environment** – when facilitating BYOD to provision sensitive services, the agency may adopt additional controls to ensure higher level of security, these controls may include but not limited to

4.2.12.1. Advanced network security technologies like VPN, reverse proxy, network access control etc.

4.2.12.2. Application whitelisting; allowing users to use only approved applications; or publishing corporate application store

4.2.12.3. Different levels of user profiles (or containers) based on job function or risk associated with access of systems and/or data

5. Implementation and Compliance

This policy is mandatory for all government agencies and recommended for organizations identified as Critical Sector Organizations.

5.1. Implementation Schedule:

5.1.1. This policy is effective from the date of publication.

5.1.2. All agencies shall complete and submit the questionnaire (Appendix D of this document) to Cyber Security Division, MOTC (cspolicy@ict.gov.qa) within a month of publication of this policy.

5.1.3. All agencies adopting BYOD after the date of publication should adopt this policy during the assessment and implementation phase.

5.1.4. Existing agencies who have already adopted the BYOD should define a roadmap to comply within six months of publication of this policy and endeavor to achieve compliance within a year of publication of this policy.

5.2. Compliance

5.2.1. Each Agency shall:

5.2.1.1. Conduct an internal self-assessment and report on its level of conformance with this policy to MOTC (cspolicy@ict.gov.qa) on an annual basis; and, Any exception or non-applicability of clause must be justified with reasonable explanation and approved by head of agency

5.2.1.2. In cases of any non-conformance to any clause of this policy, the agency must submit a Corrective and Preventative Action Plan (CAPA) detailing the mitigation measures, associated timelines and person accountable to complete..

5.2.1.3. The self-assessment report along with the action plan shall be signed by the Head or Deputy Head of the agency.

5.3. Policy Exemption

5.3.1. Any Government Agency that would like to exempt itself from the application of this policy shall submit a formal request seeking exemption providing therwith reasons for the request to to Cyber Security Division, MOTC (cspolicy@ict.gov.qa).

6. Appendix A: Factors to be considered for choosing BYOD

The Agency shall conduct the necessary due diligence and risk assessment to assess the need to use the devices not owned and managed by the agency and the applicable ownership model that they would like to adopt. On a minimum the assessment shall be guided by the following factors:

6.1. Legal and Regulatory Requirements: The management shall take into consideration the compliance of applicable laws and regulations in State of Qatar. Usage of devices that are not owned and managed by the agency may impact the state of compliance within the agency. MOTC has issued a number of policies aligned to Qatar's Cyber Security Strategy that may have a bearing on the decision (Refer Appendix E). E.g. Cloud Security Policy for Government sector. Lastly, the agency might have an existing contractual agreements with external entities that may restrict the use of devices not owned and amanaged by the agency.

6.2. Information Security Concerns (Especially Data Leakage and Loss): The decision shall weigh the heightened risk and exposure on account of usage of devices that are not owned and managed by the agency. The agency must implement baseline controls detailed in NIA 2.0 policy and further conduct formal risk assessment to implement reasonable additional controls to protect agency's data.

6.3. User Privacy Concerns: There may be concerns of privacy since the devices that are not owned and managed by the agency will have personal information (data, messages, pictures, videos etc.) that may be exposed to IT support staff (for lack of sufficient controls) or may be at risk of loss of data in case the device is sanitized. These concerns need to be adequately addressed by the management. Agency must explain the risks to privacy and secure formal consent from user before enabling devices not owned and managed by the agency.

6.4. IT Infrastructure overhead: Management should take into consideration the IT infrastructure overhead that it may entail to enable the devices that are not owned and managed by the agency. Some of the factors to consider are increased support staff with multiple skills to support multiple devices of different types owned by the employees. The requirement for additional security infrastructure such as Enterprise Mobility Management solution, etc.

6.5. Enterprise IT exposure: Management should take into considerations the enterprise IT applications that will be made available on the devices that are not owned and managed by the agency.

6.6. User experience and expected productivity gains: One key benefit attributed to the flexible ownership model (BYOD, CYOD) is the enhanced user experience and satisfaction and the associated productivity gains.

6.7. Manageability: Management should take into consideration on how the devices will be managed, the security controls that can be / will be implemented to manage agency's data

7. Appendix C: Risk Assessment

Agencies shall conduct a Risk Assessment and identify the threats and vulnerabilities to agency's information systems and corporate date due to usage of devices that are not owned and managed by the Agency.

Agencies are encouraged to adopt the National Information Risk Framework being developed by MOTC.

In carrying out the Risk Assessment, agencies should consider the following on a minimum:

Risks	Threats	Vulnerabilities	Risk Mitigation
Disclosure of sensitive Information and communication in public domain / non trusted users	Device Lost, Device Theft, Data Leakage, Employees, Improper decommissioning of devices	No secure / strong passwords, no encryption, No Procedures or Non Adherence to Procedures	Encryption of Data, Remote Wipe Capability, Access Control on device and Robust/Automated deprovisioning procedure.
Data Corruption of government records / systems	Malicious Actors, Malicious Applications, Malwares	Unpatched system & applications, Jailbroken or Rooted OS, Untrusted Applications	Use of legitimate OS, Use of Patched systems and Endpoint security.
Device Compromise to launch other attacks	Malicious Users / Attackers	Jailbroken or rooted OS, Vulnerable Applications, Malicious Applications	Use of legitimate OS, Use of Patched systems and Endpoint security.
Unavailability of Information to render government services / or to take decisions.	Device Loss, Media Corruption	Improper Physical controls, Improper maintenance	Backup of Data at regular intervals to resume services ASAP
Breach of User's Privacy	IT Support,	No proper compartmentalization, Admin Privilege misuse	Use of proper compartmentalization.

8. Appendix D: Questionnaire

1. As an organization do you allow access to corporate information from devices that are not owned and managed by the agency (e.g. USBs, phones, tablets)?:
2. If answer to question 1 was "NO", do you intend to provide access to devices that are not owned and managed by the agency?
    a. Planning within the next 12 months
    b. Part of our 3 year Plan
    c. Not in the foreseeable future

Note:

Answer to Q1	Answer to Q2	Go To
Yes	NA	Question 3
No	A or B	Answer questions from 3 – 9 from a planning perspective in terms of the factors you are considering….
No	C	Question 10

3. Was the access provided after doing due diligence by the management? If yes can you provide evidence?
4. Is there a formal policy / governance for managing the devices that are not owned and managed by the agency?
5. On what devices is the access provided on?
    a. Devices owned and managed by the Agency
    b. Devices owned but not managed by the Agency
    c. Devices not owned but managed by the Agency
    d. Devices not owned and not managed by the Agency
6. What kind of devices are supported by your organizations? E.g. USBs, portable routers, telecom devices, laptops, tablets etc
7. Does your organization restrict access to specific brands / models of supported devices? E.g. Only Tablets from Apple / Samsung will be supported.
8. If the response to Question 7 was Yes, Please list them.
9. What kind of risks have you considered in context of devices that are not owned and managed by the agency? Please list them.
10. What are list of controls that you have implemented for devices that are not owned and managed by the agency? Tick the appropriate controls: Please list if you have provided other / additional controls:
    a. Issued BYOD Security Policy and acknowledged by users.
    b. Created awareness amongst users.
    c. Process to register / de-register such devices prior connecting them to controlled network.
    d. End Point security software
    e. Strong PIN / Password
    f. Use of VPN to connect to corporate network.
    g. Compartmentalization of Data
    h. Encryption of Data
    i. Sandboxing of applications
    j. Enterprise wide Enterprise Mobility Management Suite

k. Procedures for data sanitization, media disposal and destruction.
l. Others _____

11. I hereby confirm that the answers provided above are correct to the best of my knowledge and ability.

Name of Signatory: _____

Signature: _____

Date: _____

9. Appendix E: List of relevant Legislations and Policies issued by MOTC

1. Proposed Data Privacy Law
2. National Information Assurance Policy Ver 2.0
3. Cloud Security Policy Ver 1.0
4. Blackberry Security Policy
5. Proposed National Information Risk Framework
6. Proposed iOS Security Policy
7. Proposed Windows Mobile Security Policy

The above is a list of policies issued by MOTC, there may be other regulations / policies issued by the sector regulator and / or other ministries that may be applicable in this context. Example the Cyber Crime Law issued by the Ministry of Interior.

Agencies should contact their legal department and confirm on the applicable legislations, regulations policies etc.

In case of conflicts, agencies are advised to apply the stringest of controls.

10. Appendix F: Template Acceptance Form

The following template is indicative and should be customized to suit the agency's needs.

ACCEPTANCE OF BYOD Security POLICY*
I acknowledge that I have read, understood and agree to the requirements of <agency>'s BYOD Security policy. I understand that using my personal device with <agency> data and for <agency> work purposes is an option offered by the <agency> and is not obligatory. I understand the privacy concerns and provide my assent to this information being collected by the system, having being assured that this information will only be used for work related purposes and as per the applicable regulations within the State of Qatar. I understand the minimum device requirements as applicable are set out by the agency. I accept that <title of the responsible person> at <agency> will decide whether my device meets those requirements. I also understand that the minimum device requirements may be subject to change at any time and that it is my responsibility to remain informed. I undertake to ensure that my device and the agency's information therein is appropriately secured from loss, theft or use by unauthorized persons. I also agree that the agency (relevant department) will have limited access / authority over the device for the sole purpose of protecting government/agency data and access on the device. This authority includes permission to install controls to secure and manage the device including the authority to wipe the device in the event of loss, incident or disposal as per the Agency's media sanitization and disposal policy. I acknowledge that I am responsible for replacing, maintaining and obtaining technical support for my device; except in the case of applications that <agency> has provided. I understand that access to <agency>'s systems and data is provided at the sole discretion of <agency> and may be revoked at any time and for any reason. I confirm that I have read and understood the terms of this acceptance form and the requirements of <agency's BYOD Security policy> and I will ensure that I adhere to these conditions at all times. **Signature:** ……. **Name (print):** ……. **Employee No.** ……. **Date:** …….

11. Appendix G: Accepted Device List

<This is neither an exhaustive nor the recommended list. Agencies should adjust to reflect their local requirements>

The following device types are acceptable for registration on <agency>'s Bring Your Own Device mobility service:

Mobile Phones and Smartphones

Accepted Device Types	• Apple iPhone <4s> or later • Blackberry • HTC • Nokia • Samsung • Sony
Accepted Operating System Versions	• Apple iOS version <iOS 7> or later • Windows Phone <8.1> • Android Version <4.0> or later • Blackberry OS Version <10> or later
Unaccepted Devices and Operating System Versions	Unlisted makes of mobile phone and smartphone handsets

Tablets

Accepted Device Types	• Apple • Samsung • ASUS • Microsoft
Accepted Operating System Versions	• Apple iOS version <iOS 7> or later • Windows Phone <8.1> • Android Version <4.0> or later
Unaccepted Devices and Operating System Versions	Unlisted makes of tablets

Wearable Devices

Accepted Device Types	• iWATCH • Samsung GEAR
Accepted Operating System Versions	
Unaccepted Devices and Operating System Versions	