QNREN Security Policy

Background

1. It is QNREN policy, that the private network for education and research will be most effective if it places as few technical restrictions as possible on the development or use of new applications and services. The imposition of mandatory access control or monitoring systems is likely to cause problems for existing uses of the network as well as limiting future developments, and should only be considered where there is a clear benefit.

    The public Internet network, if provided by QNREN, will have restrictions placed on the network in line with Qatar national law and MICT Qatar recommendations. This restriction can be lifted through the appropriate application process to MICT Qatar.

    Filtered or restricted network access to other destinations may be offered as optional services that organisations can join, however the core QNREN service should provide as open a network as is possible while meeting operational and legal requirements.

2. A presumption of openness brings associated risks that security incidents or misuse will seriously damage the effectiveness of the network (a summary of these risks can be found in Annex A). The impact of incidents may rapidly spread far beyond the individual organisation, machine or user where they originate. These risks must be managed if the network is to fulfil its purpose. The QNREN network has therefore adopted this Security Policy to protect the network and the organisations that use it. Under the Terms for the Provision of the QNREN Service, compliance with this Policy is a requirement for all organisations connected to the network. The Policy also places responsibilities on users of the network. The authority of QNREN, as service provider, to protect the operation of the network is established in the Terms for the Provision of the QNREN Service.

3. This QNREN Security Policy therefore has a number of goals:

    *   To ensure that appropriate local policies exist to protect QNREN, the networks connected to QNREN and the computer systems using QNREN from abuse (whether defined in this or other QNREN Policies);

    *   To ensure that mechanisms exist to aid the prevention and identification of abuse of the QNREN network;

    *   To ensure an effective response to complaints and queries about real or perceived abuses of the QNREN network;

    *   To ensure that the reputation of QNREN is protected and that the network can meet its legal and ethical responsibilities with regard to its connectivity to the worldwide Internet.

Definitions

4. The term 'User Organisation' has the meaning defined in the Terms for the Provision of the QNREN Service.

5. The term 'Connected Organisation' means any organisation with a connection to the QNREN network, whatever type of licence covers the connection. In particular it includes User Organizations.

The Policy

Responsibilities

6. The Terms for the Provision of the QNREN Service place responsibilities on every person and organisation involved in the use or operation of QNREN to protect the network against security breaches. In particular:

- Each User Organisation must ensure that all use of QNREN by those individuals and Connected Organisations to whom it provides network access complies with this Security Policy and the QNREN Acceptable Use Policy. The User Organisation must also ensure that information about security issues can be communicated rapidly within the organization and to QNREN and that problems are resolved promptly (see paragraphs 7 and 8);

- Each Connected Organisation, including those that are User Organisations, must ensure that its actions and those of the users for which it is responsible are safe for themselves and do not present a threat to others (see paragraph 9);

- Each user of the QNREN network and the networks of Connected Organisations must behave in accordance with this Security Policy and with any policies and procedures local to the Connected Organisation. The user must cooperate with their organisation and the network operators to reduce security risks;

- QNREN must ensure that the operation of the network is appropriately monitored, that the response to security problems is coordinated, and that temporary or permanent measures are implemented, up to and including disconnection, where necessary to protect the network or to comply with the law (see paragraph 10).

Points of Contact at the User Organisation

7. The successful prevention of security incidents and prompt resolution of those that do occur both depend critically on the rapid and accurate transfer of information between QNREN Connected Organizations and QNREN as operator of the network. To this end each User Organization must provide QNREN with up-to-date details of one or more persons who will act as Security Contact(s) for the User Organisation and any other organisations and individuals to whom the User Organisation provides access to QNREN. The User Organisation must ensure that its designated Security Contact(s) have appropriate knowledge, skills, resources and authority to fulfil their role (see note 1).

8. The Security Contact(s) have roles in both the prevention and resolution of security incidents:

- To disseminate QNREN's warnings of general risks and precautions to appropriate people within the organisation(s) for which they are responsible, and to ensure that appropriate preventive measures are taken promptly;

- To ensure that any particular security breach or risk that has been reported to the Security Contact(s) by QNREN as affecting an organisation for which they are responsible is investigated and resolved promptly, and to inform QNREN that this has been done.

Responsible Action by the Connected Organisation

9. Each Connected Organisation must act responsibly to protect the network. This duty includes:

- Taking effective measures to ensure that there is no security threat to QNREN or other Connected Organisations from insecure devices connected to the Organisation's network (see note 2);

- Taking effective measures to protect against security breaches, in particular ensuring that recommended security measures are implemented;

- Taking effective measures to ensure that security breaches can be investigated and that other users of the network are protected from the consequences of breaches;

- Assisting in the investigation and repair of any breach of security;

- Promoting local policies in support of this QNREN Security Policy, backed by adequate disciplinary and other procedures for enforcement;

- Implementing appropriate measures for giving, controlling and accounting for access to QNREN, backed by regular assessments of the risks associated with the measures chosen (see note 3);

- Taking reasonable measures to encourage its users to act responsibly in compliance with this Policy and the QNREN Acceptable Use Policy, and ensuring that they are enabled to do so through systems, procedures and training that support good security practice.

Monitoring and Enforcement by QNREN

10. The Terms for the Provision of the QNREN Service authorize QNREN, as the service provider responsible for the QNREN network, to require connected organisations to comply with this Policy, to monitor the network where it has reason to believe there has been a breach of the Policy or other threat, and to take such actions as are necessary to protect the operation of the network and the security of services provided to QNREN customers. In particular QNREN is authorized to:

- Monitor use of the QNREN network, while respecting privacy and national law, either in response to information about a specific threat or generally because of the perceived situation;

- Implement such temporary technical measures as are required to protect the network or its customers against breaches of security or other incidents that may damage the network's service or reputation;

- Require a User Organisation, through its nominated contact, to fulfil its responsibilities under any of the QNREN Policies;

- Where a User Organisation is unable or unwilling to co-operate, initiate the process for achieving an emergency disconnection;

- Where permitted or required by law, assist law enforcement authorities in their investigations concerning the QNREN network.

Explanatory Notes

1. Further details of the role of the Security Contact can be found by approaching QNREN technical staff or material published on the QNREN website.

2. The security of networked devices may, for example, be managed by a combination of direct configuration and maintenance, technical controls such as firewalls or router access control lists, system monitoring or probing, and delegation to appropriately skilled others. Where an organisation allows a device it does not own or control to connect to the network it is strongly recommended that consent to these normal operational measures be obtained as a condition of connection.

3. Further information about granting and accounting for access can found by approaching QNREN technical staff or material published on the QNREN website.

Appendix A: Risks to Networks and Networked Systems

All computer networks are exposed to threats, both internally and from the other networks to which they connect. Hostile traffic, both random and directed, is now a constant feature of the Internet. The particular open character of an education and research network increases both its exposure to these threats and the potential damage to the integrity and effectiveness of the network.

The risks to the network, the computers and organisations connected to it, include:

- Breaches of confidentiality. Organisations hold and have access to large amounts of intellectual property, both their own and licensed from others: the value of such property may be greatly reduced if it is disclosed to others. Organisations also handle a great deal of personal information about individuals who may suffer if it is not kept confidential: consequences range from a loss of privacy to partial or complete theft of identity.

- Loss of integrity. Information held on computers can be destroyed or modified, and unauthorised changes may be undetectable. The integrity of computers themselves may be compromised if intruders are able to take control of them, thus casting doubt on the accuracy of any results and the privacy of any data. Repeated failures can result in users losing confidence in computer systems at their own or other organisations.

- Failures of availability. Networks and the computers connected to them may be temporarily disabled either deliberately or accidentally by large flows of network traffic, making them unusable at critical times. Organisations that lose the confidence of others may find themselves unable to communicate if they are placed in a blacklist. Network and computer staff may be unavailable for support or development activities if they have to spend their time dealing with security incidents.

- Damage to reputation. The reputations of QNREN and the organizations and individuals connected to it may be seriously harmed by security incidents or inappropriate use of the network. Many intruders like to advertise their successes, others may attack third parties using computers connected to QNREN and to which they have gained control. Organisations whose systems are used in these ways are likely to be held responsible. The use of QNREN to disseminate unwanted, offensive or illegal material is also likely to be seen as misuse of a publicly-funded resource.

- Legal action. National and international law is increasingly concerned with data networks and is placing a growing list of obligations on those who provide them. Individuals, organisations and network operators who, by action or inaction, fail to meet their legal obligations may be punished by the criminal law, have substantial financial damages awarded against them or be required to modify or cease their networking operations.

The openness of QNREN and other connected networks may allow the impact of a security breach to spread far beyond an original insecure system or action. The same openness means that it will rarely be possible to protect organisations and users against the immediate consequences of their insecure actions: more often it will be necessary to respond promptly to security breaches by isolating the systems and organisations affected until the problem has been resolved.