IT Security Policy

Crown Oil
Fuels and Lubricants

1 Introduction

1.1 Purpose
The purpose of this document is to define the Crown Group information security policy.

1.2 Intended audience
It is intended to be read by employees, suppliers and customers of the Crown Group.

1.3 Overview
Data is considered a primary asset for the Crown Group. Dependence on information systems and the data held within those systems creates vulnerability for our organisation and those that we represent. Our security policy therefore focuses on controlling authorised access to data.
Security compromises or privacy violations could:

- Reduce credibility and reputation with our customers, shareholders and partners
- Violate business contracts, trade secrets, and customer privacy
- Cause loss of revenue through fraud or destruction of proprietary or confidential data
- Jeopardise our ability to provide service

1.4 Supporting Policies
Alongside the information security policy there are a further 2 more documents, the email policy and the internet policy.

2 Access control

The standard authentication policy at the Crown Group is for local authentication to be password based and remote authentication to be password & key based.

Access to the network, servers and systems is achieved by individual and unique logins, and requires authentication and authorisation.

Crown Group insists that all users of systems that contain high risk or confidential data must utilise a ‘strong password’, the definition of which is a password that is at least 12 characters consisting of upper case, lower case, and special characters and cannot contain 3 consecutive characters of the user name. User passwords resets every 60 days.

If default passwords are provided, users are forced to change these on their first successful attempt to log in and access the system. Whenever a system is installed, rebuilt or configured the Administrator or root account responsible will use a password that conforms to the Crown Groups password selection criteria.

Logins and passwords are only coded into programs or queries when they are either encrypted or otherwise secure.

Access rights of terminated employees or employees on notice period are reviewed on notice of suspension of employment and on the day of leaving. Access rights are reviewed and adjusted as necessary. All employees have their accounts and access rights disabled upon termination of employment at the Crown Group.

All system-level passwords (e.g. root, enable, administrator, application administration accounts, etc.) are changed on a regular basis, Crown Group system administrators enforce password changes every 2, 4, 6, and 12 months depending on the system and level of access. In the event that the Crown Group is aware that a password has been compromised, password change is mandatory and with immediate effect.

Only the IT Support department has full administrative rights to any Crown Group owned server storing or transmitting sensitive or client specific data.

3 Network security

It is standard Crown Group practice that all servers housed within the Crown Group environment that are Internet or public facing are firewalled and secured by using up-to-date firewalls and/or Cisco routers. Security access alerts are emailed to all I.T. support staff by the Internet facing server to warn of any unauthorised access attempts from the Internet.

Crown Group firewalls restrict traffic in both directions by default, allowing trusted/ authorised inbound traffic to a DMZ only (not the LAN), with egress filtering being employed for outbound traffic; internal security is taken as seriously as any external threat when determining security policy.

Any dormant accounts are removed from machines and file permissions are as restrictive as is practical so that security works on a “least privilege” basis.

Access control lists exist on all routers to prevent unauthorised access and logging is enabled where appropriate (deny rules for example).

All systems connected to the Internet have their security software updated regularly. System integrity checks of host and server systems housing confidential Crown Group data are performed on a regular basis and in any event at least every 6 weeks. Crown Group regularly undertakes a review of external attempts to access the system and logs all such events.

Any visitor to Crown Group is not permitted to connect any device directly into the local area network or is given access to a machine that allows them direct access to the local area network unless full authorisation has been given by the IT manager.

Crown Oil use an external contractor to preform quarterly vulnerability scans. The report is sent directly to the IT Manager. Any actions raised in the report are dealt with immediately.

4 Data transport

Any Crown Group owned laptop will not be carried outside of Crown Group premises unless it has been encrypted by the IT department and a Yubikey is provided. This then enables 2 stage authentication to access the laptop, a password alongside the Yubikey.

PCs and laptops are all governed by a domain group policy which prevents users from saving data on a removeable device which is plugged into the computer, this includes USB sticks, mobile telephones etc. This rule is lifted for some users only by authority of the IT manager.

5 Physical access

The server rooms at Crown Group contains environmental & security measures to protect essential information processing equipment. This includes separately monitored and controlled air conditioned units, smoke alarms directly linked to the buildings security monitoring systems. Permission must be requested from a member of the Network Administration Team prior to any entry/work being carried out in the server room.

All essential server room equipment / servers are connected to a UPS devices to maintain essential operation during the event of a power failure.

Entry to the main building is limited by the use of a key fob. Entry to each of the office floors is also limited by a further key fob enabled door.

6 Disaster recovery

All essential Crown Group data and source code of the suite of Crown Group software products are backed up on a daily basis to multiple locations and sites.

Backups of key servers are stored on removable storage (RDX drives) and are stored in alternate buildings.

Key servers in each of the Crown Group companies exist in a virtual environment, each virtual server is replicated to another building to allow for resilience and redundancy. See Crown Oil IT Disaster Recovery Plan for more detail

7 Virus prevention

The wilful introduction of computer viruses or disruptive/destructive programs into the Crown Group environment is strictly prohibited.

All computers have industry standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files are kept up-to-date via automatic updates and through the interventions of the Network Administration team. Virus-infected computers are removed from the network until they are verified as virus-free.

Any activities with the intention to create and/or distribute malicious programs into Crown Group network (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.

Crown Group security is not dependent upon external security policies. Although it is expected that remote nodes connecting are up-to-date, it is pragmatic to treat both authorised/prohibited connections with the different but rigid security policies.

8 Acceptable use

Crown Group computer resources are used in a manner that complies with Crown Group policies and furthermore applicable laws and regulations. Uses that interfere with the proper functioning or the ability of others to make use of the Crown Group networks, computer systems, applications and data resources are not permitted.

Decryption of passwords is not permitted, except by authorised staff performing security reviews or investigations. Use of network sniffers is restricted to system administrators who must use such tools to diagnose network problems. Auditors or security officers in the performance of their duties may also use them. They are not used for eavesdropping except under exceptional circumstances.