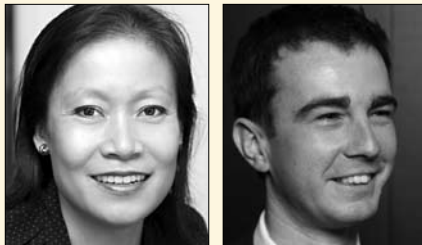


Developments in the information security landscape in the UAE



By Joycia Young and Benjamin Smith

Businesses and governments collect, store and process increasing amounts of information. That information is often highly confidential, sensitive and sometimes business critical. This update addresses legislative developments that came into force on October 29th, 2013 and regulate information security in federal authorities in the UAE.

Securing information from unauthorised, or unlawful, access, use, modification, disclosure or harm is a priority for governments and businesses alike. Our increasing reliance on sophisticated IT solutions makes securing that information more challenging than ever before. Having recognised these challenges, government departments in the UAE are taking steps to bolster internal information security measures. In recent years, each of the governments of Abu Dhabi and Dubai have implemented their own Emirate-specific information security policies. Information security measures are now being formalised at a federal level with the passing into law, on 29 October 2013, of UAE Cabinet Resolution No. 21 of 2013 (the Resolution) which regulates information security in federal authorities in the UAE.

The Resolution applies to 'the ministries, public corporations, institutions and public bodies affiliated to the federal government'. This will include ministries, such as the UAE Ministry of Economy, and other federal government departments such as the UAE Central Bank.

The objectives of the Resolution include, among other things:

- raising awareness about information security;
- setting standards for the use of IT systems; and
- ensuring that employees of federal authorities are aware of their obligations with respect to the use of IT systems.

The Resolution largely follows the form of an acceptable use policy, as opposed to placing an obligation on government departments to implement their own information security policies which adhere to certain standards or delegating responsibility for regulating information security at the federal level to a particular government department.

Different sections of the Resolution set out requirements for the use of different electronic communication methods, hardware, software and

other aspects of the federal government's IT infrastructure. By way of example, sections of the Resolution set out requirements for:

- the use of email, including on mobile devices;
- password creation;
- the use of the internet;
- anti-virus controls;
- accessing email through mobile phones;
- encryption; and
- data storage.

The Resolution also identifies four classes of confidential information ('very confidential', 'confidential', 'restricted' and 'public'). It then places an obligation on federal authorities to classify information in accordance with the four classes and to define the rights of users to access, modify, delete, copy, send or print that confidential information accordingly. This approach to classifying sensitive confidential information is a more sophisticated approach to dealing with data than is commonly prescribed in other federal legislation in the UAE.

Individual employees who breach the Resolution's requirements may be subject to criminal liability under UAE law and the disciplinary penalties that apply within the federal authority for which he or she works. The criminal liability could include both financial penalties and imprisonment.

The Resolution is the latest addition to a series of information security focused policies and laws, including government specific information security policies in Abu Dhabi and Dubai, and federal cybercrimes legislation.

Many businesses in the region are also looking to implement, or improve, acceptable use policies restricting the use of IT systems by employees. It is appropriate for acceptable use policies in a corporate environment to address many of the issues raised in the Resolution, although there a number of additional points that could also be addressed, including setting guidelines for the use of personal devices for business purposes and social media.

Clyde & Co LLP

PO Box 7001, Rolex Tower
Sheikh Zayed Road, Dubai
United Arab Emirates

Tel: (971) 4 384 4000

Fax: (971) 4 384 4004

Email: joycia.young@clydeco.com

ben.smith@clydeco.com

www.clydeco.com