Remote Access Security Policy

1) **Wireless Access Points**
Where the network is accessed remotely via wireless appropriate wireless security standards will be used.

- Wired Equivalency Protocol (WEP) will be used as standard on Wi-Fi connections.
- A WEP encryption key will be used.
- The network will be configured not to advertise its presence.
- The power of access points will be turned down to a minimum that still allows the access point to function.
- Due to the possibility of cracking Wireless Encryption Protocol using sniffing software such as AirSnort all wireless access points will be outside the firewall.
- Wi-Fi Protected Access (WPA) will be used where it is available.

2) **Secure Access via VPN**
Access from remote users to the corporate network will be via secure IPSEC VPN or SSL VPN connections only. This is necessary to secure the connection from the remote device to the corporate network.

3) **Prevention of Data Loss**
All laptops and tablets's that are taken off site will have the following security configured, to prevent data loss in the event of theft.

- The hardware password will be enabled if available.
- All corporate data on the laptop or tablets will be encrypted using appropriate encryption software.
- Sensitive documents should be accessed remotely and only downloaded if essential.

4) **Remote Device Protection**
To prevent remote PC's, laptops, PDA's etc from compromising the corporate network, security software will be installed on the devices.

- Firewall software will be installed on the devices to prevent them from being compromised by trojans and back door software.
- Anti-virus software configured to automatically download the latest virus signatures will be installed and utilised.

5) **Blue Tooth**
To prevent Bluetooth enabled devices from being attacked and compromised the Bluetooth connections on mobile phones, PDA's and laptops will be disabled where appropriate. This is to prevent bluejacking, SNARF and backdoor attacks.

6) **Standard Devices & Configurations**

Devices that are used to access the network remotely, must meet the minimum standard for supported web browsers and operating systems, that is current at the time of access.

Where access is provided directly to the corporate network, users will only be allowed access on standard devices authorised and approved by corporate ICT Services.

7) **Authentication**

Authentication for remote access will use two-stage authentication. As a minimum this will comprise two-stage username and password verification.

Where possible to enhance the authentication of users one of the following additional methods of authentication will be used in conjunction with the users password.

- Digtal Certificate
- Smart Card
- SecureId Card

8) **Hardened Corporate Applications**

All corporate applications will be hardened as much as possible, particular attention will be paid to those applications, which are accessible remotely. The security features of applications will be fully utilised and all security patches will be applied.

9) **Working Outside the UK**

a) Laptops / Tablets / Vasco
Council IT equipment including laptops and tablets and may not be taken outside of the boundaries of the United Kingdom.

b) Mobile Phones
Council Mobile Phones may be taken outside of the boundaries of the United Kingdom. This feature will be initially disabled, and can be activated by contacting the Councils Telecoms Provider before leaving the UK. Users will be responsible for any personal calls and data usage.

c) Users are not permitted to access Council data from outside the United Kingdom.