Security guidance against fraudulent use of one communications system/Voice Mail system

The following notes are provided as guidance to best practice in setting up and managing your telephone system in the interests of reducing exposure to fraudulent use.

1. The DISA/IDD service should only be allocated to authorized members of staff on a “genuine need” basis.

2. Access to the DISA/IDD service should be restricted by password (authorization code).

3. An individual password for DISA/IDD access should be allocated to each authorized staff member.

4. DISA/IDD passwords should contain a minimum of 4 digits and should be changed every three months.

5. Telephone extension numbers, and staff or ID numbers, should not be used as DISA/IDD passwords.

6. Discourage staff from writing down their passwords and access numbers.

7. Ensure that staff sign non-disclosure agreements in relation to their Keyline system passwords.

8. VoIP service should only be allocated to authorized members of staff on a “genuine need” basis.

9. Monitor usage of chargeable telephone calls, such as IDD calls and Infoline.

10. Install an IDD call accounting system to monitor daily/weekly telephone calls on the one communications System to ensure IDD calls are for genuine business use.

11. Limit the number of DISA trunk lines to facilitate monitoring of DISA usage.

12. Activate time duration and destination barring (optional) for DISA/IDD calls, if facilities are available with the system.

13. A voicemail user should set password for his/her mailbox and change it periodically.

14. If a voicemail or voice response system is installed on the one communications system, then prevent these systems from transferring callers to make IDD calls at your company’s cost.

15. Immediately cancel the DISA/IDD and voicemail password of any staff member who leaves the company.

16. Restrict access to the one communications system equipment room to authorized persons.

17. Physical access to the one communications system programming port should be restricted to those persons authorized by your company. Access to the programming port should be by password only.

18. The main unit should not be placed in a public area, as this increases risk of unauthorized access.

The above guidance is given in good faith for your general information only. You are advised to develop your own safety measures to prevent possible fraudulent use of Voice Mail and DISA/IDD service.