AD HOC TASK GROUP
[DATA]
31 July - 4 August 2006
Manila, Philippines

RULES AND PROCEDURES FOR THE SECURITY OF MEDIUM RISK DATA HELD BY THE WCPFC

WCPFC/AHTG [Data]/2006/06

Paper prepared by the Secretariat

1. The Second Session of the Commission adopted a recommendation to establish an ad hoc Task Group [AHTG] (Data) to identify types of data that must be treated as confidential and to develop draft rules and procedures to govern the security and confidentiality of data collected and held by the Commission.

2. In support of the work of the AHTG (Data), the Secretariat, in collaboration with members of the Scientific Committee's Statistics Specialist Working Group (S-SWG), circulated the following draft documents on 6 April 2006 for comment:

- Draft Rules and Procedures for the Security of Data held by the WCPFC;
- Draft Principles and Procedures for Dissemination by the Commission of Fisheries Compliance Data; and
- Draft Principles and Procedures for the Dissemination of Scientific Data by the Commission.

3. Comments on the above drafts were received from Members by 31 May 2006. The attached document (Appendix A) has been prepared in response to those comments for the consideration of the AHTG (Data).

Appendix A

DRAFT

RULES AND PROCEDURES FOR THE SECURITY OF MEDIUM RISK DATA HELD BY THE WCPFC

Version 1.0
[July 2006]

Western and Central Pacific Fisheries Commission
PO Box 2356
Kolonia 96941
Pohnpei State
Federated States of Micronesia

Rules and procedures for the security of medium risk data held by the WCPFC

Background

In August 2005 the Scientific Committee of the WCPFC recommended that the Commission establish an ad-hoc task group to:

- Identify types of data that must be treated as confidential; and
- To develop draft rules and procedures to govern the security and confidentiality of data collected and held by the Commission.

In December 2005 this recommendation was accepted by the Commission.

This document describes rules and procedures for the security of medium risk data held by the Commission. Medium risk data includes operational level Catch Effort and the equivalent Observer data.

Principles

1) The Commission will use the framework provided by the international ISO17799 standard as a means to help ensure that it operates a complete set of information security measures. ISO17799 will serve as a check list for the completeness of security arrangements for data. However, it is not envisaged that the Commission will formally adopt ISO17799 to the extent that it seeks to achieve an ISO17799 certification.

2) The Commission will categorise the data that it holds in terms of level of security risk.
    a. Low security risk data will include (but are not restricted to): registrations of fishing vessels / authorisations, trade documentation scheme data, estimates of annual catches, biological data collected by observers or port sampling.
    b. Medium security risk data will include: operational level Catch Effort data and the equivalent observer data.
    c. High security risk data will include: Vessel Monitoring System data and data describing intelligence / surveillance operations.

3) The Commission will adopt information security measures appropriate to mitigate the security risks that are relevant to each category of data. In the case of medium security risk data, these risks include (but are not restricted to):
    a. A deliberate pre-planned attempt by an unauthorised person (or persons) to gain access to data. For example – an attempt to break into WCPFC data storage premises, or “hack” into WCPFC computer systems;
    b. A deliberate opportunistic attempt by an unauthorised person (or persons) to acquire and pass on (to a 3rd party) data. For example – a cleaner or contractor working on WCPFC premises picking a data CD that they found on a desk;
    c. An accidental release of operational data as a consequence of a careless act by an authorised person. For example – an obsolete computer being disposed of without first having the hard disk appropriately reformatted.

Rules and procedures

The purpose of this document is to provide a checklist for the completeness of information security arrangements for medium risk data (including operational level Catch Effort data and the equivalent observer data). This document is intended to compliment the Commission's security policy and security plan, and is not a substitute for either.

The rules and procedures that follow are intended to be read alongside the ISO17799:2001 "Code of practice for information security management" document. The ISO17799 document provides the discussion and explanation for each rule/procedure.

With regard to medium security risk data, the Commission will ensure:

The Commission's Security Policy

1 Information security policy document - There is a Commission information security policy, which is approved by the management, published and communicated (as appropriate) to all employees. It states the management commitment and sets out the organisational approach to managing information security. (ISO17799:2001 - 3.1.1)

2 Review and evaluation - The information security policy has an owner, who is responsible for its maintenance and review according to a defined review process. (ISO17799:2001 - 3.1.2)

3 Review and evaluation - The information security policy review process ensures that a review takes place in response to any changes affecting the basis of the original assessment (for example: significant security incidents, new vulnerabilities or changes to organisational or technical infrastructure). (ISO17799:2001 - 3.1.2)

The Commission's Organisational Security

4 Allocation of information security responsibilities - Responsibilities for the protection of individual information assets, and for carrying out specific security processes, are clearly defined. (ISO17799:2001 - 4.1.3)

5 Specialist information security advice - Specialist information security advice is obtained when appropriate. (ISO17799:2001 - 4.1.5)

6 Co-operation between organisations - Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators are maintained to ensure that action can be quickly taken and advice obtained, in the event of a security incident. (ISO17799:2001 - 4.1.6)

7 Independent review of information security - The implementation of the information security policy is reviewed independently on regular basis. (ISO17799:2001 - 4.1.7)

8 Identification of risks from third party access - In those cases where access to Commission information processing facilities by third parties is needed - the types of accesses needed by third parties are identified and classified. The risks associated with

this access are identified and appropriate security controls implemented. (ISO17799:2001 - 4.2.1)

9 Identification of risks from third party access - Access to information and information processing facilities by third parties is not provided until appropriate controls have been implemented. (ISO17799:2001 - 4.2.1)

10 Security requirements in third party contracts - Arrangements involving third party access to organisational information processing facilities are based on a formal contract containing, or referring to, all the security requirements to ensure compliance with the organisation's security policies and standards. (ISO17799:2001 - 4.2.2)

11 Security requirements in outsourcing contracts - In cases where the Commission has outsourced the management and control of all or some of its information systems, security requirements are addressed in the contract with the third party. The outsourcing contract addresses how the legal requirements are to be met, how the security of the Commission's assets maintained and tested, and the right of audit, physical security issues and how the availability of the services is to be maintained in the event of a disaster. (ISO17799:2001 - 4.3.1)

The Commission's Information Asset Classification and Control

12 Inventory of assets - An inventory is maintained of information assets, software, hardware and supporting infrastructure (heating, lighting, power, air conditioning etc). Each asset identified has an owner, security classification and location documented. (ISO17799:2001 - 5.1.1)

13 Classification guidelines - There is an Information classification scheme or guideline in place; which assists in determining how the information asset is handled and protected. (ISO17799:2001 - 5.2.1)

14 Information labelling and handling - An appropriate set of procedures are defined for information labelling and handling; in accordance with the classification scheme adopted by the Commission. (ISO17799:2001 - 5.2.2)

The Commission's Personnel Security

15 Including security in job responsibilities - Security roles and responsibilities are documented in Commission's information security policy. This includes both general and specific responsibilities for the protection of specific assets, and the execution of particular security processes or activities. (ISO17799:2001 - 6.1.1)

16 Personnel screening and policy - Appropriate verification checks on employees are carried out at the time of job applications. For employees holding positions of considerable authority these checks are repeated at appropriate intervals. (ISO17799:2001 - 6.1.2)

17 Confidentiality agreements - Employees are required to sign confidentiality or non-disclosure agreements as a part of their initial terms and conditions of the employment. (ISO17799:2001 - 6.1.3)

18 Confidentiality agreements - Casual staff and third party users (not already covered by an existing contract) are required to sign confidentiality agreements prior to being given access to information processing facilities. (ISO17799:2001 - 6.1.3)

19 Terms and conditions of employment - The terms and conditions of the employment covers the employee's responsibility for information security. Where appropriate, these responsibilities continue for a defined period after the end of the employment. (ISO17799:2001 - 6.1.4)

20 Information security education and training - All employees of the Commission and third party users receive appropriate information security training and regular updates in organisational policies and procedures. (ISO17799:2001 - 6.2.1)

21 Reporting security incidents - There are appropriate procedures for reporting security incidents (through appropriate management channels and as quickly as possible). (ISO17799:2001 - 6.3.1)

22 Reporting security weaknesses - There are appropriate procedures for reporting security weakness in, or threats to, systems or services. (ISO17799:2001 - 6.3.2)

23 Learning from incidents - There are appropriate mechanisms in place to ensure the types, volumes and costs of incidents and malfunctions are quantified and monitored. (ISO17799:2001 - 6.3.4)

24 Disciplinary process - There are appropriate disciplinary processes for employees who violate organisational security policies and procedures. These processes act as a deterrent to employees who might otherwise be inclined to disregard security procedures. (ISO17799:2001 - 6.3.5)

The Commission's Physical and Environmental Security

25 Physical Security Perimeter - There is a physical security perimeter in place to protect areas which contain information processing facilities. (ISO17799:2001 - 7.1.1)

26 Physical entry Controls - Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access. (ISO17799:2001 - 7.1.2)

27 Securing Offices, rooms and facilities - The selection and design of secure areas takes into account the possibility of damage from natural or man-made disasters (for example: fires and floods). (ISO17799:2001 - 7.1.3)

28 Working in Secure Areas - Appropriate controls exist on the behaviour of people working within secure areas. (ISO17799:2001 - 7.1.4)

29 Equipment siting protection - Equipment is sited to minimise unnecessary opportunities for unauthorised access. (ISO17799:2001 - 7.2.1)

30 Cabling Security - Telecommunications cables carrying data or supporting information services are protected from interception. (ISO17799:2001 - 7.2.3)

31 Securing of equipment off-premises - The security provided for equipment and information while outside the premises is equivalent to that on-site (taking into account the purpose of the equipment or information, and the additional risks of working off site). (ISO17799:2001 - 7.2.5)

32 Secure disposal or re-use of equipment - During disposal or re-use, storage devices containing sensitive information are physically destroyed or securely over written. (ISO17799:2001 - 7.2.6)

33 Clear Desk and clear screen policy - An automatic computer screen locking facility is enabled. This locks the screen when the computer is left unattended for a period. (ISO17799:2001 - 7.3.1)

34 Clear Desk and clear screen policy - Sensitive material in the form of paper documents, media etc., is stored in locked cabinets/furniture when unattended (and not left sitting on desks). (ISO17799:2001 - 7.3.1)

35 Removal of property - Equipment, information or software cannot be taken off site without appropriate authorisation. (ISO17799:2001 - 7.3.2)

36 Removal of property - Equipment, information or software cannot be removed from a secure area without appropriate authorisation. (ISO17799:2001 - 7.3.2)

The Commission’s Communications and Operations Management

37 Documented Operating procedures - Operating procedures (for example: information processing/handling, contact lists in the event of difficulties, back-up, equipment maintenance etc) identified by the information security policy, are documented and maintained. (ISO17799:2001 - 8.1.1)

38 Documented Operating procedures - Changes to operating procedures are authorised by management. (ISO17799:2001 - 8.1.1)

39 Operational Change Control - Changes to information processing facilities and systems are controlled. Formal management responsibilities and procedures are in place to ensure satisfactory control of all changes to equipment, software or procedures. Operational programs are subject to strict change control. (ISO17799:2001 - 8.1.2)

40 Operational Change Control - Audit logs, recording any changes made to the operational programs, are maintained. (ISO17799:2001 - 8.1.2)

41 External facilities management - Where external contractors are used to management information - The risks associated with this have been identified in advance, and appropriate controls agreed with the contractor and incorporated into the contract. (ISO17799:2001 - 8.1.6)

42 Control against malicious software - Appropriate detection and prevention controls to protect against malicious software are implemented. Protection against malicious software is based on employee security awareness, appropriate system access and change management controls. (ISO17799:2001 - 8.3.1)

43 Information back-up - Back-up copies of essential information and software are taken regularly. (ISO17799:2001 - 8.4.1)

44 Information back-up - Adequate backup and restore facilities are provided to ensure that all essential information and software can be recovered following a disaster or media failure. (ISO17799:2001 - 8.4.1)

45 Information back-up - Backup and restore arrangements for individual systems are regularly tested to ensure that they meet the requirements of continuity plans. (ISO17799:2001 - 8.4.1)

46 Network Controls - There are appropriate controls to ensure the security of data in networks, and the protection of connected services from unauthorised access. (ISO17799:2001 - 8.5.1)

47 Management of removable computer media - There are appropriate controls on the removable of storage media such as tapes, disks, cassettes, memory cards and printed reports. (ISO17799:2001 - 8.6.1)

48 Disposal of Media - Storage media that are no longer required are disposed off securely and safely. (ISO17799:2001 - 8.6.2)

49 Information handling procedures - There are procedures for the handling and storage of information storage media (including paper copies) that protect such information from unauthorised disclosure or misuse. The procedures for the handling and storage of information are consistent with the information's security classification. (ISO17799:2001 - 8.6.3)

50 Security of system documentation - System documentation is protected from unauthorised access. (ISO17799:2001 - 8.6.4)

51 Information and software exchange agreement - Agreements exist for the exchange of information and software between organisations, where such exchange is needed. Security issues are documented in these agreements, and reflect the sensitivity of the information involved. (ISO17799:2001 - 8.7.1)

52 Security of Media in transit - Appropriate controls exist to safeguard information when being transported between sites. (ISO17799:2001 - 8.7.2)

53 Security of Electronic mail - A clear policy exists regarding the use of electronic mail. Appropriate controls exist to reduce the security risks created the use of by electronic mail (for example: viruses, interception or misdirection of unencrypted email). (ISO17799:2001 - 8.7.4)

54 Security of Electronic office systems - Policies and guidelines are implemented to control the security risks associated with electronic office systems. (ISO17799:2001 - 8.7.5)

55 Publicly available systems - There is a formal authorisation process in place for the promotion of information onto publicly available systems. (ISO17799:2001 - 8.7.6)

56 Publicly available systems - Software, data and other information requiring a high level of integrity, made available on a publicly available system, is protected by appropriate mechanisms. (ISO17799:2001 - 8.7.6)

57 Other forms of information exchange - There is a clear policy statement for the procedures staff are expected to follow in the use of voice, facsimile and video communication facilities. Procedures and controls are in place to protect the exchange of information through the use of voice, facsimile and video communication facilities. (ISO17799:2001 - 8.7.7)

The Commission's Access Control

58 Access Control Policy - There is an access control policy describing how robust access controls need to be, and addressing the rules and rights for each group of users. (ISO17799:2001 - 9.1.1)

59 User Registration - There is a formal user registration and de-registration procedure for granting access to multi-user information systems and services. (ISO17799:2001 - 9.2.1)

60 Privilege Management - The allocation and use of privileges in multi-user information system environment is restricted and controlled through a formal authorization process. (ISO17799:2001 - 9.2.2)

61 User Password Management - The allocation and reallocation of passwords is controlled through a formal management process. (ISO17799:2001 - 9.2.3)

62 User Password Management - Passwords are not stored on computer systems in an unprotected form. (ISO17799:2001 - 9.2.3)

63 Review of user access rights - There is a process to review user access rights at regular intervals. (ISO17799:2001 - 9.2.4)

64 Password use - Users follow appropriate security practices in the selection and use of passwords. (ISO17799:2001 - 9.3.1)

65 Unattended user equipment - Employees and contractors are made aware of security requirements and procedures for protecting unattended equipment. (ISO17799:2001 - 9.3.2)

66 Policy on use of network services - Users are only provided with direct access to information and services that they have been specifically authorised to use. (ISO17799:2001 - 9.4.1)

67 Policy on use of network services - A policy exists concerning access to networks and network services. (ISO17799:2001 - 9.4.1)

68 Enforced path - There are controls that restrict the route between a user terminal and the information services its user is authorised to access (creating an enforced path). (ISO17799:2001 - 9.4.2)

69 User authentication for external connections - Access by remote users is subject to appropriate authentication. (ISO17799:2001 - 9.4.3)

70 Node Authentication - Connections to remote computer systems that are outside Commission's security management are authenticated. (ISO17799:2001 - 9.4.4)

71 Remote diagnostic port protection - Access to diagnostic ports is securely controlled. (ISO17799:2001 - 9.4.5)

72 Network connection control - Appropriate controls to restrict the connection capability of users are implemented. Such controls are based on the access control policy and requirements of applications, and are maintained and updated accordingly. (ISO17799:2001 - 9.4.7)

73 Network routing control - Appropriate routing controls exist on shared networks. These controls are based on the access control policy, and on the positive source and destination address checking mechanisms. (ISO17799:2001 - 9.4.8)

74 Security of network services - The security attributes of all network services in use, or being considered for use, is documented. (ISO17799:2001 - 9.4.9)

75 Automatic terminal identification - Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment. (ISO17799:2001 - 9.5.1)

76 Terminal log-on procedures - Appropriate procedures for logging into information systems minimise the opportunity for unauthorised access. (ISO17799:2001 - 9.5.2)

77 User identification and authorisation - A unique identifier is assigned to every user for their personal and sole use. Activities can subsequently be traced to the responsible individual. (ISO17799:2001 - 9.5.3)

78 User identification and authorisation - Generic (shared) user accounts are only be supplied under exceptional circumstances where there is a clear need. Such cases are approved by management, documented, and subject to any additional controls that are appropriate to maintaining security. (ISO17799:2001 - 9.5.3)

79 Password management system - Password management systems provide an effective, interactive, facility which ensures quality passwords. (ISO17799:2001 - 9.5.4)

80 Use of system utilities - The use of system utilities programs (capable of overriding system and other application controls) is restricted and tightly controlled. (ISO17799:2001 - 9.5.5)

81 Terminal time-out - Inactive terminals in high risk areas, or serving high risk systems, shut down automatically after a defined period of inactivity. The shut down facility

clears the terminal screen and closes both application and network sessions. (ISO17799:2001 - 9.5.7)

82 Information access restriction - Users of systems (including support staff) are provided with access to information and information system functions in accordance with a defined access control policy. Access is based on individual requirements and consistent with the organisational information access control policy. (ISO17799:2001 - 9.6.1)

83 Event logging - Audit logs recording exceptions and other events relevant to security are produced and kept for an appropriate period. (ISO17799:2001 - 9.7.1)

84 Clock synchronisation - Where a computer or communication device has the capability of operating a real time clock, it has been set to an agreed standard such as Universal co-ordinated time or local standard time. There is a procedure that checks for and corrects any significant variation in clock time. (ISO17799:2001 - 9.7.3)

85 Mobile computing - There is an appropriate policy on working with mobile computing facilities (laptops, notebooks, palmtops etc), especially in unprotected environments. The policy includes appropriate requirements for physical protection, access controls, cryptographic techniques, back-ups and viruses protection. (ISO17799:2001 - 9.8.1)

86 Mobile computing - Appropriate protection is in place to avoid unauthorised access to, or disclosure of, information processing facilities that are in public places or unprotected areas. (ISO17799:2001 - 9.8.1)

87 Mobile computing - When facilities are used in public places, appropriate care is taken to avoid the risk of overlooking by unauthorised persons. (ISO17799:2001 - 9.8.1)

88 Mobile computing - Procedures against malicious software are in place and kept up to date. (ISO17799:2001 - 9.8.1)

89 Mobile computing - Backups are adequately protected against theft or loss. (ISO17799:2001 - 9.8.1)

90 Mobile computing - Remote access to information across public networks using mobile computing facilities only takes place after successful identification and authentication, and with appropriate access control mechanisms in place. (ISO17799:2001 - 9.8.1)

91 Mobile computing - Mobile computing facilities are physically protected against theft (for example - when in cars, hotel rooms, meeting places). (ISO17799:2001 - 9.8.1)

92 Mobile computing - Equipment carrying sensitive information is not left unattended, and where appropriate is locked away, or special locks used to secure the equipment. (ISO17799:2001 - 9.8.1)

93 Mobile computing - Employees receive appropriate training in the use of mobile computing facilities to raise their awareness of the additional risks resulting from this way of working and controls that need to be implemented to mitigate the risks. (ISO17799:2001 - 9.8.1)

94 Teleworking - There is a policy to control teleworking activities, this is consistent with organisation's security policy. Teleworking is only authorised where appropriate security arrangements are in place. (ISO17799:2001 - 9.8.2)

95 Teleworking - Appropriate protection is in place, at each teleworking site, against threats such as theft of equipment, unauthorised disclosure of information, unauthorised remote access to internal systems etc. (ISO17799:2001 - 9.8.2)

The Commission's Systems Development and Maintenance

96 Security requirements analysis and specification - Security requirements are described in the specifications for new systems (or for enhancement to existing systems). Specifications describe the automated controls to be incorporated into the system, and supporting manual controls. (ISO17799:2001 - 10.1.1)

97 Security requirements analysis and specification - Security requirements are specified as part of requirement statements when evaluating software packages for purchase. Where appropriate use is made of independent evaluations and certification of security. (ISO17799:2001 - 10.1.1)

98 Policy on use of cryptographic controls - There is a policy in use of cryptographic controls for the protection of information. (ISO17799:2001 - 10.3.1)

99 Encryption - Appropriate encryption techniques are used to protect information. (ISO17799:2001 - 10.3.2)

100 Key management - A key management system is in place to support the Commission's use of cryptographic techniques. The key management system is based on a set of standards, procedures and secure methods. (ISO17799:2001 - 10.3.5)

101 Key management - All keys are protected against modification and destruction. (ISO17799:2001 - 10.3.5)

102 Key management - Secret and private keys are protected against unauthorised disclosure. (ISO17799:2001 - 10.3.5)

103 Key management - Keys have defined activation and deactivation dates so that they can only be used for a limited period of time. (ISO17799:2001 - 10.3.5)

104 Control of operational software - Appropriate controls are in place for the implementation of software on operational systems. (ISO17799:2001 - 10.4.1)

105 Control of operational software - Software patches are applied where they can help remove or reduce security weaknesses. (ISO17799:2001 - 10.4.1)

106 Control of operational software - Access to information or information systems is only been given to suppliers (for support purposes) when necessary and approved by management. The suppliers activities are monitored. (ISO17799:2001 - 10.4.1)

107 Protection of system test data - System test data is protected and controlled. The use of operational databases containing personal/sensitive information is avoided for test purposes. If such information is used, the data has been depersonalised/sensitized before use. (ISO17799:2001 - 10.4.2)

108 Access control to program source library - Strict controls are in place over access to program source libraries. (ISO17799:2001 - 10.4.3)

109 Change control procedures - These are appropriate formal change control procedures to ensure that security is not compromised, that programmers only have access to those parts of the system necessary to do their work, and formal approval for any changes is obtained. (ISO17799:2001 - 10.5.1)

110 Technical review of operating system changes - After change to operating systems, application systems are reviewed and tested to ensure that there has been no adverse impact on security. (ISO17799:2001 - 10.5.2)

111 Restrictions on changes to software packages - As far as is possible, and practical, vendor supplied software packages are used without modification. (ISO17799:2001 - 10.5.3)

112 Covert channels and Trojan code - Appropriate controls are in place to protect against trojan code and covert channels. (ISO17799:2001 - 10.5.4)

The Commission’s Business Continuity Management

113 Operational continuity management process - There is a managed process in place for developing and maintaining operational continuity throughout the organisation. (ISO17799:2001 - 11.1.1)

114 Operational continuity management process - Continuity planning identifies events that can cause disruptions to processes, and includes a risk assessment. (ISO17799:2001 - 11.1.2)

115 Writing and implementing operational continuity plan - Continuity plans have been developed to maintain or restore operations within the required time following interruption. (ISO17799:2001 - 11.1.3)

116 Writing and implementing operational continuity plan - Whether there is a single framework of continuity plans which ensures that all plans are consistent and identifies priorities for testing and maintenance.. (ISO17799:2001 - 11.1.3)

117 Operational continuity planning framework - When new requirements are identified, established emergency procedures are amended where appropriate. (ISO17799:2001 - 11.1.4)

118 Operational continuity planning framework - Each continuity plan has an appropriately empowered named owner. (ISO17799:2001 - 11.1.4)

119 Testing, maintaining and re-assessing operational continuity plan - Continuity plans are tested regularly to ensure that they are up to date and effective. (ISO17799:2001 - 11.1.5)

120 Testing, maintaining and re-assessing operational continuity plan - Continuity plans are maintained by regular reviews and updates to ensure their continuing effectiveness. (ISO17799:2001 - 11.1.5)

The Commission's Compliance

121 Safeguarding of organisational records - Cryptographic keys are protected against degradation, loss, destruction and falsification, and made available to authorised persons when needed. (ISO17799:2001 - 12.1.3)

122 Safeguarding of organisational records - Data storage systems are chosen such that data can be retrieved in a manner acceptable to a court of law. (ISO17799:2001 - 12.1.3)

123 Safeguarding of organisational records - The system of storage and handling clearly identifies records and their required retention period. (ISO17799:2001 - 12.1.3)

124 Data protection and privacy of personal information - There are management structures and controls in place to ensure compliance with data protection, and privacy of personal information, legislation. (ISO17799:2001 - 12.1.4)

125 Prevention of misuse of information processing facility - A log-on a warning message is presented on the computer screen indicating that unauthorised access is not permitted. (ISO17799:2001 - 12.1.5)

126 Compliance with security policy - Managers ensure that all security procedures within their area of responsibility are carried out correctly. (ISO17799:2001 - 12.2.1)

127 Compliance with security policy - There are regular reviews of compliance with security policies, standards and requirements. (ISO17799:2001 - 12.2.1)

128 Technical compliance checking - Information systems are regularly checked for compliance with security implementation standards. Technical compliance checks are carried out by, or under the supervision of, competent, authorised persons. (ISO17799:2001 - 12.2.2)

129 System audit controls - Audit requirements and activities involving checks on operational systems are carefully planned to minimise the risk of disruptions to operational process. (ISO17799:2001 - 12.3.1)

130 Protection of system audit tools - System audit tools (such as software or data files) are protected to prevent any possible misuse or compromise. (ISO17799:2001 - 12.3.2)