Reminder

Government of India
Ministry of Railways
(Railway Board)

No. 2005/RBCC/7/3/Policy

New Delhi dated 19-03-2007

GMs /All Indian Railways and PUs

Subject: IT Security

Ref : Earlier letter No.2006/C&IS/OTH/CERT/33 dated 06-10-2006.

In reference to above, a letter alongwith a questionnaire was sent to all zonal railways and production units to assess the status of security and level of preparedness to deal with any exigencies. The completed questionnaire was to reach this office by 15th November 2006. The questionnaire was to be sent to Department of Information Technology.

The same may please be submitted, complete in all respects, by 15th April 2007. A soft copy of the questionnaire, in MS-Word format, may also please be emailed to prog1@rb.railnet.gov.in.

DA: As above

(Amitabh Lal)
Executive Director (C&IS)

Note: Railways / Production Units who have replied to the questionnaire earlier may please ignore this letter.

Template for reporting information security policy compliance by Govt. and critical sector organizations

(In accordance with DIT's information security policy document CERT-In/NISAP/01, Iss 01, May 2006)

****

1. Name of the organization:

2. Total number of employees:

3. Percentage of employees trained in IT security awareness:

4. Number of employees with significant IT responsibility:

5. Percentage of employees under Para 4 above with specialized training:

6. Date of report:

7. Details of person (CISO) submitting the report

   - Name –
   - Designation –
   - E-mail –
   - Tel –
   - Fax -

Table A – Compliance details

The control objectives and controls listed in the following table are derived from those listed in IS/ISO/IEC 27001:2005, Clauses 5 to 15. Kindly indicate if a control is not applicable.

Security policy		
1	Does Information security policy document exist? • Indicate date of issue and version No.	
2	Is review of the information security policy done? • Frequency of review • Date of last review and • Has it considered the findings of risk assessment and residual risks?	
Organization of information security		
3	Is allocation of information security responsibilities done? • Identify the CISO (Name and designation)	
4	Is independent review/audit of information security done (including third party ISMS audits)? • Frequency of review/audits • Date of last review/audits and • By whom (identify the team or organization)? *Ref. CERT-In empanelled List of IT security auditors at www.cert-in.org..in* • Are all corrective actions complete following the audit?	
Asset management		
5	Is there an Inventory of all information and information processing assets (Includes IT hardware, software and information assets)?	
6	Is the Ownership of such assets clearly identified?	
7	Are there information classification guidelines?	
8	Are guidelines available for information labelling and handling?	
Human resources security		
9	Do the terms and conditions of employment clearly state the IT security related responsibilities?	

10	Are access rights removed soon after an employee ceases to be on rolls? • Indicate Av. Time for removal of access rights	
Physical and environmental security		
11	Are secure physical entry controls enforced?	
12	Are equipment appropriately sited and protected?	
Communications and operations management		
13	Are third party services Monitored and reviewed?	
14	Is use of resources monitored and projections made of future capacity requirements to ensure the required system performance?	
15	Are controls against malicious code implemented? • Indicate Av. Time for virus updates	
16	Are Controls against mobile code implemented?	
17	Are back-up copies of information and software taken and tested regularly in accordance with the backup policy? • Indicate frequency of back-ups	
18	Are appropriate network and web security guidelines implemented? *Ref. CERT-In web security guidelines at* www.cert-in.org.in	
19	Are audit logs recording user activities, exceptions, and information security events produced and kept for an agreed period to assist in future investigations and access control monitoring.	
20	Is there a mechanism to monitor IT system use? Indicate • The frequency of such reviews and • Date of last review	
21	Are logging facilities and log information protected against tampering and unauthorized access.	
Access control		
22	Is there an access control policy?	
23	Is there a review of user access rights? Indicate • Frequency of such reviews • The date of last review	

24	Password use – Indicate the minimum length of passwords	
Information systems acquisition, development and maintenance		
25	Is software development in-house or outsourced? Are secure development guidelines followed? Ref www.oqasp.org for guidelines on secure web application development	
26	Are timely information about technical vulnerabilities obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk? Indicate • Av. Security patch latency (time between patch release and deployment)	
Information security incident management		
27	Reporting information security events – Indicate the following: • Total No. of incidents • No. of incidents reported internally • No. of incidents reported to CERT-In • No. of incidents reported to law enforcement agencies • No. of incidents before security audit • No. of incidents after security audit • No. of incidents of root compromise • No. of incidents of user compromise • No. of incidents of denial of service attack • No. of incidents of web defacement • No. of incidents of detection of virus/malicious logic • No. of incidents of successful virus intrusion	
Business continuity management		
28	Is there a business continuity plan based on risk assessment? • Indicate the date of last review	
Compliance		
29	Are all relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements explicitly defined, documented, and kept up to date for each information system and the organization?	

30	Are data protection and privacy ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses?	
31	Technical compliance checking – • Are Information systems regularly checked (Penetration test/Vulnerability assessment/Application security audit etc) for compliance with security implementation standards? *Ref. www.sans.org for updated information on current top vulnerabilities in windows systems and Unix systems* • Frequency of such audits? • Indicate the date of last audit • By whom (identify the team or organization)? *Ref. CERT-In empanelled List of IT security auditors at www.cert-in.org.in* • Are all corrective actions complete following the audit?	