GOVERNMENT OF INDIA
MINISTRY OF RAILWAYS
(RAILWAY BOARD)

No.2012/RBCC/7/7/Cyber-Security

New Delhi, Dated 02/07/2012

The General Managers
All Indian Railways,
Core & Production Units

Director General
RSC, Vadodara
RDSO, Lucknow

CAO
COFMOW,DMW/Patiala

Directors,
All Centralised Training Institutes

Managing Director,
Centre for Railway Information Systems,
Chanakyapuri, New Delhi.

Sub: Review of IT security measures on Railway Units.

IT security policy for Railway Units has been issued by Board in 2008. Copy of the same is available on the website of Railway Board(C&IS Dt.).

As per the said policy, each railway unit has to nominate IT security manager to look after and manage the requirements pertaining to the same. To emphasise on the importance of IT security and ensure that relevant issues are addressed in right earnest, a review meeting of all nominated IT security managers is scheduled at Railway Board as per details below:

Date	:	**19th July 2012**
Time	:	**10.00 hrs.**
Venue	:	**Conference Hall, 2nd Floor, Rail Bhawan**

The nominated IT security managers of each railway units may come prepared with a presentation highlighting the status and action taken on their railway units, with respect to the issues indicated in the annexure. For clarifications please contact the undersigned (dmecis@rb.railnet.gov.in) or Sh. Yogesh Katyal, Programmer, Railway Board Computer Centre (prog2@rb.railnet.gov.in, 9717635887)

Later on another meeting shall be scheduled and intimated to the Railway Units, wherein a review would be done in Board with AGMs or SDGMs (where AGMs are not in place). For Production Units and CTI etc. where AGM and SDGM are not in place, the IT incharge (at least SAG) would be called for the said review.

The above has the approval of Board (MT, CRB).

DA: As above

(Suyash Narain)
Director ME(C&IS)

Annexure

Silent Features of IT security policy

i. Zonal Railways/ PU should set up their own IT Security Organization that includes one or more IT Security managers, Incident response team and IT Security monitoring team.

ii. Contingency management planning should be in place in case of emergency/ disaster in mission critical application / information. Backup policy should also be taken into consideration while drafting the contingency management planning

iii. Licensed Software need to be used in all the systems/ applications. The patch management system should be in place for timely updation of all licensed softwares. The updation of software is must to plug any vulnerability in software.

iv. Password management policy should be framed in detail using combination of special characters etc. The password should be disclosed only to authentic users.

v. Developers, while designing the application, should plan security framework. Version control mechanism should be in place. Documentation and listing of application should be in safe custody.

vi. In order to protect system, network etc from virus, malicious codes, spam etc. anti virus software alongwith firewall, IDS must be installed in every system. If possible, a central anti virus server may be installed and each system should be scanned centrally. All latest definitions should be pushed through central server.

vii. In order to implement IT Security policy, Zonal Railways/ Production Units are advised to procure and install only licensed software. You are also advised to procure and install antivirus software, patch management software etc. The financial implication of procurement and the renewal of software license may be charged in revenue.

viii. All running applications and network should be security audited by third party vendors. The list of vendors is available at CERT-In website i.e. http://cert-in.org.in/

ix. Any Other issue relevant to the subject in accordance with the IT Security policy.

Note : The above are features of the IT security policy in brief. For clarifications and further details, please consult the policy.