



Government of Haryana/ हरियाणा सरकार
Secretariat for Information Technology
सूचना प्रौद्योगिकी सचिवालय

From

Financial Commissioner & Principal Secretary to Govt. Haryana,
Electronics & Information Technology Department,
Chandigarh.

To

All Administrative Secretaries,
All Divisional Commissioners,
All Heads of Departments,
All Chief Executives of Boards,
Corporations, Agencies & Authorities and
All Deputy Commissioners of the Haryana State.

Memo No.: 4/153/1190

Dated: 21-04-2010

Subject: Crisis Management Plans for Countering Cyber Attacks and Cyber Terrorism.

The Department of Information Technology (DIT), Govt. of India has prepared a Crisis Management Plan for countering Cyber Attacks and Cyber Terrorism, which was endorsed by the National Crisis Management Committee (NCMC). DIT, GoI has requested to draw-up sectoral Crisis Management Plan for countering Cyber Attacks & Cyber Terrorism and take necessary steps to plan and implement the same.

In view of the above, I am directed to request you to get the Crisis Management Plan prepared, in case your department/organization has sensitive/vital data and to take the action on following points:

1. Identify Critical Information assets and implement Department's information Security Policy to secure these.
2. Prepare an organizational level Crisis Management Plan (CMP) on the lines of CMP of CERT-In, outlining roles & responsibilities of organizational stakeholders and CMP coordination process.
3. To develop and implement the CMP on the lines of CMP of CERT-In and report compliance on a periodic basis.
4. Identify a member of senior management as a 'Chief Information Security Officer (CISO)' to coordinate security policy compliance efforts across the department and interact regularly with CERT-In and state level 'Point of Contact'.
5. Establish a Crisis Management Group, with HoD as its Chairman.



Government of Haryana/ हरियाणा सरकार
Secretariat for Information Technology
सूचना प्रौद्योगिकी सचिवालय

6. Prepare a list of contact persons with up-to-date contact details with respect to information security and CMP.
7. Implement the CMP, including security best practices and organisation's Information Security Policy.
8. Identification of all critical ICT assets, functions and Information assets across the departments. Consolidation of all critical information assets. The information assets, which need to be protected from various departments, should be covered under CMP.

For any further details, guidance, technical assistance or advice, you may contact Sh. Satyender Kumar, STD, NIC-HSU at satyen@hry.nic.in / 0172-2741950 or Sh. Pardeep Kaushal, PSA, NIC-HSU at p.kaushal@nic.in / 0172-2741950 with details of critical IT assets and implementation details of organization's Information Security Policy, within 10 days. A softcopy of the documents on Crisis Management Plan prepared by DIT, Gol and Template for preparing the CMPs is also available with them.

Anam Bansal.
Manager(IT)

for Financial Commissioner & Principal Secretary to Govt. Haryana,
Electronics & Information Technology Department