

प्रेषक,

आयुक्त एवं सचिव,
राजस्व परिषद, उ० प्र०,
कम्प्यूटर सेल, लखनऊ।

सेवा में,

समस्त जिलाधिकारी,
उत्तर प्रदेश।

संख्या: १०० / 1-18-2010/क०सेल/विविध/०९

दिनांक 12 अगस्त 2010

विषय: काइसिस मैनेजमेंट प्लान एण्ड स्टैण्डर्ड प्रोसिजर्स के सम्बन्ध में।

महोदय,

आप अवगत हैं कि प्रदेश के समस्त जनपदों में चकबन्दी प्रक्रिया से बाहर के समस्त ग्रामों की खतौनियों को शत-प्रतिशत कम्प्यूटरीकृत किया जा चुका है तथा "उत्तर प्रदेश अधिकारों का अभिलेख (कम्प्यूटरीकरण) नियमावली, 2005" के द्वारा कम्प्यूटरीकृत खतौनी उद्घरण को विधिक मान्यता प्रदान की जा चुकी है। प्रदेश की समस्त तहसीलों में भू-अभिलेखों की कम्प्यूटरीकरण योजना के अन्तर्गत कम्प्यूटर केन्द्र की स्थापना भी करायी जा चुकी है। कम्प्यूटरीकृत खतौनी का डाटा तहसील कम्प्यूटर केन्द्र में स्थापित कम्प्यूटर्स पर उपलब्ध है। इसके अतिरिक्त अन्य महत्वपूर्ण डाटा भी तहसीलों में उपलब्ध है, यथा-प्रमाण-पत्रों का डाटा भी उपलब्ध है। उक्त डाटाबेस की सुरक्षा अति आवश्यक है। डाटाबेस की सुरक्षा के लिये समय-समय पर परिषद स्तर से दिशा-निर्देश निर्गत किये गये हैं।

2. मुख्य सचिव, उत्तर प्रदेश शासन के स्तर से निर्गत आई०टी० एवं इलेक्ट्रॉनिक्स विभाग के शासनादेश सं०-863/78-1-2010-05आईटी-1/05, दिनांक 24 मई 2010 के द्वारा डाटाबेस की सुरक्षा के लिये निम्नलिखित निर्देश दिये गये हैं-

2.1. प्रत्येक कम्प्यूटर पर लीगल ऑपरेटिंग सिस्टम तथा सिस्टम साफ्टवेयर का ही प्रयोग किया जाय। किसी भी दशा में पायरेटेड साफ्टवेयर का प्रयोग दण्डनीय होगा। प्रत्येक ऑपरेटिंग सिस्टम को क्रमिक रूप से अपडेट किया जाय।

2.2. प्रत्येक कम्प्यूटर पर एन्टी वायरस लोड किया जाय तथा इसे क्रमिक रूप से अपडेट किया जाय।

2.3. सिस्टम पर जो भी पासवर्ड बनाया जाय वह पासवर्ड नीति के अन्तर्गत हो जिसमें कम-से-कम एक कैपिटल लेटर, एक स्मॉल लेटर, एक न्यूमरिक तथा एक स्पेशल करैक्टर का होना अनिवार्य तथा पासवर्ड कम-से-कम 8 करैक्टर को हो।

2.4. यूजर अपना पासवर्ड किसी भी दशा में किसी दूसरे के साथ शेयर न करे जिस कारण से कभी भी साइबर अटैक की कोई क्षति होती है तो उसका उत्तरदायित्व संबंधित

यूज़र का होगा। उपरोक्त के अतिरिक्त विभाग से संबंधित भारत सरकार द्वारा प्रेषित टेम्पलेट के आधार पर काइसिस मैनेजमेंट प्लान तैयार करके आईटी0 एवं इलेक्ट्रॉनिक्स विभाग को उपलब्ध कराने की अपेक्षा की गयी है।

उल्लेखनीय है कि तहसील कम्प्यूटर केन्द्र में स्थापित कम्प्यूटर्स हेतु उक्त बिन्दु सं0-2.1 व 2.2 के संबंध में तहसील कम्प्यूटर केन्द्र से प्रयोक्ता प्रभार के रूप में प्राप्त हो रही धनराशि से तहसील कम्प्यूटर केन्द्र के साफ्टवेयर के अद्यतनीकरण हेतु दिशा-निर्देश क्रमशः परिषदादेश सं0-1494/-1-18-2008/क0सेल/32/2008, दिनांक 25-11-2008 व सं0-1106/1-18-2009/क0सेल/10/2004टी0सी0-2, दिनांक 04-8-2010 के द्वारा निर्गत किये जा चुके हैं।

उपर्युक्त के सम्बन्ध में उक्त शासनादेश की छायाप्रति संलग्न कर प्रेषित करते हुये मुझे यह कहने का निदेश हुआ है कि कृपया तदनुसार कार्यवाही सुनिश्चित करने का कष्ट करें।

संलग्नक: यथोक्त।

भवदीय,

(विशाल भारद्वाज)

सहायक भूमि व्यवस्था आयुक्त,
कृते आयुक्त एवं सचिव।

संख्या व दिनांक उपर्युक्त।

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित-

1. समस्त मण्डलायुक्त, उत्तर प्रदेश को उक्त शासनादेश की छायाप्रति सहित इस आशय के साथ प्रेषित कि कृपया अपने मण्डल के समस्त जनपदों/तहसीलों में तदनुसार कार्यवाही सुनिश्चित कराने का कष्ट करें।
2. उप सचिव, उत्तर प्रदेश शासन, राजस्व अनुभाग-4, को उनके पत्र सं0-1230/1-4-10-66बी-4/10, दिनांक 14 जून 2010 के क्रम में।

आज्ञा से,

(विशाल भारद्वाज)

सहायक भूमि व्यवस्था आयुक्त,

1230/1-110
66B-4/10
81/1

शीर्ष प्राथमिकता
संख्या-863/78-1-2010-05आईटी-1/05

प्रेषक,

अतुल कुमार गुप्ता,

मुख्य सचिव

उ०प्र० शासन

सेवा में,

समस्त प्रमुख सचिव/सचिव,

उत्तर प्रदेश शासन ।

टी० एवं इलेक्ट्रॉनिक्स अनुभाग-1

1104/JSD/18
मेघव्यूग
LS(NS) 1504

28-05-10
2-06-10
J.S.

लखनऊ: दिनांक: 24 मई, 2010

विषय:-आईसिस मैनेजमेन्ट प्लान एण्ड स्टैण्डर्ड प्रोसिजर्स के सम्बन्ध में ।

महोदय,

(d) आप अवगत है कि वर्तमान में विश्व के विभिन्न भागों से हैकर्स द्वारा विभिन्न प्रकार के साईबर काईम व डाटा हैकिंग की जा रही है, जिससे लगभग सभी शासकीय विभागों को डाटा सिक्योरिटी के लिए खतरा उत्पन्न हो गया है। इस समस्या से निपटने के लिए आई०टी० एवं इलेक्ट्रॉनिक्स विभाग के पत्र संख्या-भा.स.-22/78-1-2010-05आई०टी०-1/05, दिनांक 24 मई, 2010 द्वारा विस्तृत गाईड-लाईन्स तथा राज्य के लिये तैयार किये गए साफ्ट काईसिस मैनेजमेन्ट प्लान प्रेषित किए जा चुके हैं जिसके आधार पर विभागों को भी अपने काईसिस मैनेजमेन्ट प्लान तैयार कर अन्य कार्यवाही की जानी होगी। साईबर सिक्योरिटी हेतु निम्न कदम उठाये जाने आवश्यक हैं:-

- (1) प्रत्येक कम्प्यूटर पर लीगल आपरेटिंग सिस्टम तथा सिस्टम साफ्टवेयर का ही प्रयोग किया जाए। किसी भी दशा में पायरेटेड साफ्टवेयर का प्रयोग दण्डनीय होगा। प्रत्येक आपरेटिंग सिस्टम को कमिक रूप से अप-डेट किया जाए।
- (2) प्रत्येक कम्प्यूटर पर एण्टी-वायरस लोड किया जाए तथा इसे कमिक रूप से अप-डेट किया जाए।

24 मई
21-मई
03-6-10

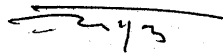
का कोई भी पक्ष किसी न्यायालय स्वयंसेवक से अन्तरण करने के लिये अन्तरण किया जा सकता है।

- (3) ~~यदि~~ ~~अलग-अलग~~ अन्य सिस्टम में जो भी पासवर्ड बनाया जाए वह पास नीति के अन्तर्गत हो, जिसमें कम से कम एक कैपिटल लेटर, एक स्माल लेटर, एक न्यूमेरिक तथा एक स्पेशल कैरेक्टर का होना अनिवार्य है तथा पासवर्ड कम से कम 8 कैरेक्टर का हो। उदाहरण स्वरूप aBmn2\$xy
- (4) यूजर अपना पासवर्ड किसी भी दशा में किसी दूसरे के साथ शेयर न करें। इस कारण से यदि कभी भी साईबर अटैक के कोई क्षति होती है तो उसका उत्तरदायित्व सम्बन्धित यूजर का होगा।

इसके अतिरिक्त भारत सरकार ने काईसिस मैनेजमेन्ट प्लान बनाने हेतु कुछ विस्तृत दिशा-निर्देश भेजे हैं जिसकी प्रति संलग्न है तथा पूर्व में आई. टी. के उक्त संदर्भित पत्र दिनांक 8.05.10 द्वारा प्रदेश के लिये तैयार गये ड्राफ्ट काईसिस मैनेजमेन्ट प्लान की प्रति के साथ प्रेषित की जा चुकी है, जिसके आधार पर सभी विभागों को काईसिस मैनेजमेन्ट प्लान बनाकर उपलब्ध कराना है।

उपर्युक्त के सम्बन्ध में अपेक्षा है कि आप अपने विभाग से सम्बन्धित भारत सरकार द्वारा प्रेषित टैम्पलेट्स के आधार पर काईसिस मैनेजमेन्ट प्लान तैयार करके प्रत्येक दशा में दिनांक 25.05.10 तक आईटी0 एवं इलेक्ट्रानिक्स विभाग को उपलब्ध करा दिया जाए। यदि किसी विभाग के डाटा सिक्योरिटी की हैकिंग के कारण किसी प्रकार की क्षति होती है और उस विभाग का काईसिस मैनेजमेन्ट प्लान नहीं बना है तो इसका सम्पूर्ण उत्तरदायित्व विभाग का होगा।

भवदीय



(अतुल कुमार गुप्ता)
मुख्य सचिव

Organisational CMP – Suggested points for action to be taken by Critical Sector Organisations

- Identify a member of senior management as a 'Chief Information Security Officer (CISO)' to coordinate security policy compliance efforts across the organisation and interact regularly with CERT-In and sectoral 'Point of Contact'
- Establish a **Crisis Management Group**, on the lines of Sectoral Crisis Management Committee, with head of organisation as its Chairman
- Prepare a list of contact persons complete with up-to-date contact details
- Prepare an **Organisational level CMP** on the lines of CMP of CERT-In, outlining roles, responsibilities of organisational stakeholders, CMP coordination process
- **Implement the CMP**, including security best practices and specific action points as outlined below:
 - Prepare a **Security plan** and implement Security control measures as per **ISO 27001 standard** and other guidelines/standards as appropriate
 - Carry out **periodic IT security risk assessments** and determine acceptable level of risks, consistent with business impact assessment and criticality of business functions
 - Develop and implement a **business continuity strategy** and **contingency plan** for IT systems
 - Develop and implement **ICT disaster recovery** and **security incident management processes**

- Periodically test and evaluate the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks and it can include:
 - Penetration testing (both announced and unannounced)
 - Vulnerability assessment
 - Application security testing
 - Web security testing
- Carry out audit of information infrastructure on an annual basis and when there is a major upgradation/change in IT infrastructure, by an independent IT security auditing organisation (Ref. to list of CERT-In empanelled IT security auditors on CERT-In web site at <http://www.cert-in.org.in>)
- Report to CERT-In cyber security incidents as and when they occur and status of cyber security periodically and take part in cyber security mock drills
- Participate in the cyber security drills to be conducted by CERT-In on a regular basis