संख्या:-1016/**78-1-2024-1099/434/2019**

प्रेषक,

अनिल कुमार सागर,

प्रमुख सचिव,

उ0प्र0 शासन।

सेवामें,

समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव,

उ0प्र0 शासन।

आई0टी0 एवंइलेक्ट्रानिक्स अनुभाग-1 लखनऊः दिनांक 09 जुलाई, 2024

विषयःस्टैण्डर्ड ऑपरेटिंग प्रोसिज़र (एस0ओ0पी0) का अनुपालन किये जाने के सम्बन्ध में।

महोदय,

उपर्युक्त विषयक के संबंध में अवगत कराना है कि प्रदेश सरकार के विभिन्न विभागों द्वारा, विगत् वर्षों में कोर आई0टी0 एवं ई-गवर्नेन्स इन्फ्रास्ट्रक्चर को विकसित किया गया है, जिसका उपयोग कर आम जनमानस द्वारा सरकारी सेवाओं का लाभ इन्टरनेट के माध्यम से लिया जा रहा है, जिसके परिणामस्वरूप साइबर स्पेस में साइबर अटैक्स की सम्भावनायें भी प्रबल हो गयी है। इस संवेदनशील डाटा की वृद्वि निरन्तर हो रही है तथा इसके उपयोग एवं आदान-प्रदान में भी वृद्वि हो रही है, जिस हेतु इस संवेदनशील डाटा एवं एप्लीकेशन की सुरक्षा करना अत्यन्त आवश्यक हो गया है।

2- भारत सरकार द्वारा महत्वपूर्ण/संवेदनशील डाटा तथा एप्लीकेशनन्स की सुरक्षा के दृष्टिगत इन्फॉरमेशन सिक्योरिटी एक्ट-2000 की धारा 70ए के अन्तर्गत नेशनल क्रिटिकल इन्फॉरमेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेन्टर (एन0सी0आई0आई0पी0सी0) संस्था का गठन किया गया है, जिसे क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर के संरक्षण के संबंध में राष्ट्रीय नोडल एजेंसी के रूप में नामित किया गया है। यह संस्था क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर को सुरक्षा प्रदान करने की दिशा में कार्य करता है। एन0सी0आई0आई0पी0सी0 के प्राथमिक कार्यों जैसे-साइवर हमलों के विरूद्व महत्वपूर्ण बुनियादी ढांचों को सुदृढ़ करना, वेनराबिलिटी एनॉलिसिस, इन्सीडेन्टरिस्पॉन्स और कैपेसिटी बिल्डिंग सम्मिलित है।

3- एन0सी0आई0आई0पी0सी0 उत्तर प्रदेश राज्य के शासकीय विभागों की महत्वपूर्ण वेबसाईट्स/वेब एप्लिकेशन की नियमित निगरानी तथा सुरक्षा ऑडिट करता है। इसके साथ ही एन0सी0आई0आई0पी0सी0 राज्य के चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर्स (सी0आई0एस0ओ0) के साथ प्रभावित वेबसाईट/वेब एप्लिकेशन की भेद्यता (वेनराबिलिटी) रिपोर्ट भी साझा करता है, ताकि समय रहते वेनराबिलिटी का निदान करते हुए इसे साइबर हमले से सुरक्षित किया जा सके।

4- आई0टी0 एवं इलेक्ट्रानिक्स अनुभाग-1, उ0प्र0 शासन द्वारा शासनादेश सं0-843/78-1-2024-1099/86/202024 दिनांक 29 मई, 2024 के माध्यम से वेबसाईट/वेब एप्लिकेशन की

भेद्यता (वेनराबिलिटी) का ससमय निस्तारण किये जाने हेतु समस्त विभागों को निर्देश जारी किये गये है।

5- साइबर वेनराबिलिटी विभागीय पोर्टल तथा इससे सम्बन्धित Third Party Installed Software में हो सकती है। वेबसाईट/वेबपोर्टल को डेवलप तथा होस्ट करने में कई Third Party Software का प्रयोग निम्नवत् किया जाता है:-

i. Windows/Linux for Operating System
ii. MSSQL/Oracle/MYSQL/Postgres for Database
iii. JBoss/Tomcat/IIS/Nginx etc. for Web/Application Server
iv. Third Party Libraries like TextSharp, Rest Client, SSRS etc.

6 - NCIIPC द्वारा समय-समय पर उपरोक्त वर्णित विभागीय पोर्टल तथा Third Party Software के किसी विशेष वर्ज़न में वेनराबिलिटी रिपोर्ट की जाती है , जिसका ससमय समाधान अत्यन्त आवश्यक है। इसी क्रम में साफ्टवेयर में प्राप्त वेनराबिलिटी के त्वरित समाधान हेतु State Level Application Information Repository बनाया जाना प्रस्तावित है, जिसके लिए विभागों द्वारा विभागीय पोर्टल से सम्बन्धित डाटा (प्रारूप संलग्न) साझा किया जाना अपेक्षित है।

7- इस संबंध में मुझे यह कहने का निदेश हुआ है कि उपरोक्त डाटा को श्री नवनीत कुमार राय, वरिष्ठ सलाहकार, स्टेट ई-गवर्नेन्स मिशन टीम (एस.ई.एम.टी.), उ0प्र0 (मोबाइल नम्बर-8284865020) के ई-मेल- navnit.rai@semt.gov.in पर शीघ्रातिशीघ्र उपलब्ध कराये जाने हेतु सम्बन्धित को कृपया निर्देशित करने का कष्ट करें।

<u>**संलग्नकः यथोक्त।**</u>

भवदीय,

Signed by
Anil Kumar Sagar **(अनिल कुमार सागर)**
Date: 08-07-2024 11:47:40 प्रमुख सचिव

<u>संख्या-1016(1)/78-1-2024 तद्दिनांक</u>

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषितः-

1-निजी सचिव, मुख्य सचिव, उ0प्र0 शासन।

2-निजी सचिव, अपर मुख्य सचिव, मा0 मुख्यमंत्री जी, उ0प्र0।

3-निजी सचिव, कृषि उत्पादन आयुक्त, उ0प्र0।

4-निजी सचिव, अवस्थापना एवं औद्योगिक विकास आयुक्त, उ0प्र0।

5-राज्य समन्वयक, सीईजी. लखनऊ।

6-गार्डफाइल।

आज्ञा से,

Signed by
Neha Jain (नेहा जैन)
विशेष सचिव।
Date: 08-07-2024 18:09:39

Department of IT & Electronics, Govt. of UP

Details of Installed Third Party Software's Components

Instruction: *You are hereby requested to follow the following instructions before proceeding further:*

1) This data will play a crucial role to address the upcoming vulnerabilities w.r.t. your Department, Technical Partner and installed software components.
2) All the information are mandatory. Please coordinate with your technical partner to fill this form.
3) Section 1- will contain organization details. Officer in charge for IT related work or CISO details shall be provided under officer name. Also Provide the Technical Partner details.
4) Section 2- will contain the application details. If a department has more than one application then all the application details shall be provided. Currently, two sets (2) are given to provide two application details. Department may create additional set as needed.

Section 1: Organization Details

Department	
Agency/ Corporation if any	
Officer Name (Preferably CISO)	
Designation	
Mobile	
Email	
Technical Partner (Pls Select who is developing agency of the Application)	NIC/ Vendor/ Department itself
Vendor Name (if selected Vendor)	
Technical Officer Name	
Designation	

Mobile	
Email	

Section 2: Department Application Details

Department Application - 1			
Name of Application			
URL			
Hosting Info (SDC/ Cloud) Please specify the Hosting name if other than SDC			
Security Audit		Yes / No	
Security Audit Expiry Date (dd/mm/yyyy) if selected Yes			
Installed Third Party Software			
1.1	**Details of installed Operating System**		
OS Name		Version	
Original Equipment Manufacturer (OEM)			
1.2	**Details of installed Database**		
DB Name		Version	
OEM			
1.3	**Details of Framework/ Technology/Library Used**		
1.3.1	Name		
	Version		
	OEM		
1.3.2	Name		
	Version		
	OEM		

Department of IT & Electronics, Govt. of UP

<table>
<tr><td colspan="5">Department Application - 2</td></tr>
<tr><td colspan="3">Name of Application</td><td colspan="2"></td></tr>
<tr><td colspan="3">URL</td><td colspan="2"></td></tr>
<tr><td colspan="3">Hosting Info (SDC/ Cloud)
Please specify the Hosting name if other than SDC</td><td colspan="2"></td></tr>
<tr><td colspan="3">Security Audit</td><td colspan="2">Yes / No</td></tr>
<tr><td colspan="3">Security Audit Expiry Date (dd/mm/yyyy) if selected Yes</td><td colspan="2"></td></tr>
<tr><td colspan="5">Installed Third Party Software</td></tr>
<tr><td>2.1</td><td colspan="4">Details of installed Operating System</td></tr>
<tr><td colspan="2">OS Name</td><td></td><td>Version</td><td></td></tr>
<tr><td colspan="3">Original Equipment Manufacturer (OEM)</td><td colspan="2"></td></tr>
<tr><td>2.2</td><td colspan="4">Details of installed Database</td></tr>
<tr><td colspan="2">DB Name</td><td></td><td>Version</td><td></td></tr>
<tr><td colspan="3">OEM</td><td colspan="2"></td></tr>
<tr><td>2.3</td><td colspan="4">Details of Framework/ Technology Used</td></tr>
<tr><td rowspan="3">2.3.1</td><td colspan="2">Name</td><td colspan="2"></td></tr>
<tr><td colspan="2">Version</td><td colspan="2"></td></tr>
<tr><td colspan="2">OEM</td><td colspan="2"></td></tr>
<tr><td rowspan="3">2.3.2</td><td colspan="2">Name</td><td colspan="2"></td></tr>
<tr><td colspan="2">Version</td><td colspan="2"></td></tr>
<tr><td colspan="2">OEM</td><td colspan="2"></td></tr>
</table>