संख्याः-843/78-1-2024-1099/86/202024

प्रेषक,

अनिल कुमार सागर,
प्रमुख सचिव,
उ0प्र0 शासन।

सेवा में,

समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव,
उ०प्र० शासन।

आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-1 **लखनऊः दिनांकः २१ मई,2024**

विषयः-प्रदेश में साइबर सिक्योरिटी के दृष्टिगत "साइबर सिक्योरिटी एडवाइज़री-एन०सी०आई० आई० पी०सी० एडवाइजरी" के सफल क्रियान्वयन एवं कुशल संचालन हेतु Standard Operating Procedures (SOPs) विषयक।

महोदय,

उपर्युक्त विषय के संबंध में अवगत कराना हैं कि प्रदेश सरकार के विभिन्न विभागों द्वारा विगत् वर्षों में कोर आई०टी० 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 अटैक्स् की सम्भावनायें भी प्रबल हो गयी है। इस संवेदनशील डाटा की वृद्धि निरन्तर हो रही है तथा इसके उपयोग एवं आदान-प्रदान में भी वृद्धि 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 एप्लीकेशनन्स् की सुरक्षा के दृष्टिगत इन्फॉरमेशन सिक्योरिटी एक्ट 2000 की धारा 70ए के अन्तर्गत National Critical Information Infrastructure Protection Centre (NCIIPC) संस्था का गठन किया गया है, जिसे Critical Information Infrastructure (CII) के संरक्षण के संबंध में राष्ट्रीय नोडल एजेंसी के रूप में नामित किया गया है। यह संस्था देश एवं प्रदेशों में विभिन्न विभागों द्वारा स्थापित Critical Information Infrastructure को सुरक्षा प्रदान करने की दिशा में कार्य कर रहा है। NCIIPC के प्राथमिक कार्यों जैसे साइबर हमलों के विरूद्ध महत्वपूर्ण बुनियादी ढांचों को सुदृढ़ करना, Vulnerability Analysis, Incident Response and Capacity Building इत्यादि सम्मिलित है।

3- अवगत कराना है कि NCIIPC उत्तर प्रदेश राज्य के शासकीय विभागों की महत्वपूर्ण वेबसाईट्स / वेब एप्लीकेशन की नियमित निगरानी तथा सुरक्षा ऑडिट करता है। इसके साथ ही NCIIPC राज्य स्तरीय चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर्स (CISO) के साथ प्रभावित वेबसाईट/वेब एप्लीकेशन की Vulnerability Report भी निरंतर अंतराल पर सॉझा करता है, ताकि समय रहते वेनराबिलिटी का निदान करते हुए इसे साइबर हमलें से सुरक्षित किया जा

सके।

4- NCIIPC संवेदनशील इन्फॉरमेशन इन्फ्रास्ट्रक्चर की साइबर सुरक्षा के दृष्टिगत निम्नलिखित श्रेणी के अन्तगर्तत एडवाइजरी जारी करता है:-

(क) विभागीय पोर्टल्स/वेबसाइट्स में प्राप्त Vulnerability हेतु एडवाइजरी।

(ख) Installed Third Party Softwares (Such as Vulnerability in MSSQL, Windows Server, MSMQ, Microsoft Azure Products, VPN, Antivirus, MySql etc.) में प्राप्त Vulnerability हेतु एडवाइजरी।

(ग) Inversion of Compromise (IOC) - Malicious URL, IPs को प्रतिबन्धित करने हेतु एडवाइजरी।

5- प्रभावित वेबसाईट/वेब एप्लीकेशन एवं Installed Third Party Software Components में प्राप्त वेनराबिलिटी के निवारण तथा उपरोक्त एडवाइज़री को प्रभावी ढंग से लागू करने हेतु निम्नलिखित Standard Operating Procedure (S.O.P) का निर्माण किया गया है, जोकि निम्नवत् है:-

(1) विभागीय पोर्टल्स/वेबसाइट्स में प्राप्त Vulnerability के समाधान हेतु S.O.P (संलग्नक-1)।

(2) Installed Third Party Softwares में प्राप्त Vulnerability के समाधान हेतु S.O.P (संलग्नक-2)।

(3) Inversion of Compromise (IOC) - Malicious URL, IPs को प्रतिबन्धित करने हेतु एडवाइजरी के क्रियान्वयन हेतु S.O.P (संलग्नक-3)।

6- राज्य के महत्वपूर्ण क्रिटिकल इन्फॉरमेशन इन्फ्रास्ट्रक्चर की सुरक्षा के दृष्टिगत उपरोक्त S.O.P का निर्माण किया गया है, जिसका अनुपालन प्रत्येक स्टेक होल्डर के द्वारा किया जाना है, जिनकी भूमिकाएं एवं उत्तरदायित्व S.O.P में उल्लिखित है। साथ ही साइबर सुरक्षा तथा एप्लीकेशन में प्राप्त वेनराबिलिटी के समाधान से सम्बन्धित किसी भी प्रकार की सहायता हेतु आई०टी० एवं इलेक्ट्रानिक्स विभाग, उ०प्र० शासन से समन्वय स्थापित किया जाये।

7- इस सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि कृपया उपरोक्त S.O.P का अनुपालन अपने-अपने विभागों में सुनिश्चित कराने का कष्ट करें।

संलग्नकः यथोक्त।

भवदीय,

Digitally Signed by (अनिल कुमार सागर)
कुमार सागर
Date: 28-05-2024 13:18:59
Reason: Approved

प्रमुख सचिव।

पृ0 संख्या-843(1)/78-1-2024, तद्दिनांक

प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित:-

1-निजी सचिव, मुख्य सचिव, उ०प्र० शासन।

2-निजी सचिव, आयुक्त, कृषि उत्पादन, उ०प्र०।

3-निजी सचिव, आयुक्त, अवसंरचना एवं औद्योगिक विकास (आई०आई०डी०सी०), उ०प्र०।

4-डी०जी०पी०, उ०प्र०।
5-राज्य, चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर्स (सी०आई०एस०ओ०), उ०प्र०।
6-एस०आई०ओ० एन०आई०सी०, उ०प्र०।
7-प्रबन्ध निदेशक, यू०पी० डेस्को।
8-राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स।
9-विभागीय, चीफ इन्फॉरमेशन सिक्योरिटी ऑफिसर्स (सी०आई०एस०ओ०), उ०प्र०।
10-हेड, एस.ई.एम.टी., उ०प्र०।
11-गार्ड फाइल।

आज्ञा से,

(नेहा जैन)

विशेष सचिव।

SoP for Implementing Cyber Security Advisory – Closing Vulnerabilities in installed Third Party Products

1. Introduction

Various third-party software applications are utilized in the development and hosting of government websites and web applications. Additionally, specific versions of some of these third-party software programs have been identified to contain critical or high vulnerabilities. It is strongly advised to promptly upgrade any existing versions of third-party software upon the discovery of critical or high vulnerabilities. NCIIPC provides information on the names and versions of such vulnerable third-party software components.

Example of some of the key Third Party Softwares:

1.	Operating System Software	Windows Server, Ubuntu, CentOS, Red Hat Enterprise Linux (RHEL), and Debian
2.	Database	MSSQL, MYSQL, PostgreSQL, ORACLE, Mongo DB, IBM DB2
3.	Application Server	Nginx, Apache. Apache HTTP Server, IIS
4.	Other Softwares	Open BI, Microsoft Azure Product, MSMQ, GitHub, Azure Kubernetes, Adobe, Siemens etc.

2. Abbreviation

S. No.	Abbreviation	Description
1	NCIIPC	National Critical Information Infrastructure Protection Centre
2	CISO	Chief Information Security Officer
3	SeMT	State e-Governance Mission Team

4	CeG	Centre for e-Governance
5	UPSDC	Uttar Pradesh State Data Center
6	SoP	Standard Operating Procedure

3. Traffic Light Protocol (TLP)

The advisory provided by NCIIPC includes a Traffic Light Protocol (TLP), which specifies the intended audience for sharing. TLP promotes enhanced information sharing by categorizing information into different levels to ensure it is shared appropriately. It utilizes four colors to denote expected sharing boundaries for the recipients. Below are the definitions of TLP levels:

TLP: Red	Not for disclosure, restricted to participants only.
TLP: Amber+Strict	Limited disclosure, restricted to participants' organization.
TLP: Amber	Limited disclosure, restricted to participants' organization and its clients
TLP: Green	Limited disclosure, restricted to the community.
TLP: Clear	Disclosure is not limited.

4. Key Stakeholders

(a) NCIIPC

(b) State CISO

(c) Department CISO

(d) Deputy CISO

(e) SeMT/ CeG Team

(f) UPSDC Team

(g) Application owner of hosted application

(h) Technical Team of respective Application

5. Step for Vulnerability Resolution in the installed third party products

1) The State CISO sends cyber security vulnerability advisories for installed components from NCIIPC to the SeMT team via email for prompt action.
2) The SeMT team informs the respective Department CISO, Deputy CISO, and UPSDC Manager about cyber security vulnerabilities in installed components. They share details such as
   - ❖ Component name
   - ❖ Version
   - ❖ Severity Level (Critical, High, Medium, Low)
3) Vulnerabilities in installed components rated as Critical/ or High severity must be resolved **within two weeks** from the reporting date to the respective department.
4) It's also recommended to update patches or versions for installed components which are rated as Medium / or Low severity level.
5) The CISO, with the help of the Deputy CISO and application owner, directs the concern team to fix the vulnerability within the set timeline (**within two weeks for Critical/ or High Severity**) and updates the concerned stakeholders (e.g., SeMT/CeG Team and UPSDC Manager/UPSDC team).
6) If the website or web application of **vulnerable installed components is hosted in UPSDC, the UPSDC Manager deactivates it if the vulnerabilities are not resolved within the given timeline.** Three reminders are sent by the UPSDC team to the application owner and other stakeholders: two reminders in the first week and one reminder in the second week.
7) The SeMT team coordinates and updates the NCIIPC about the status of vulnerability closure.

6. Role & Responsibility of Stakeholder

(a) **The State CISO** oversees and monitors the entire process of vulnerability closure.

(b) **The Department CISO** ensures that vulnerabilities are addressed within the specified timeframe.

(c) **The Deputy CISO** technically assists CISO in vulnerability closure.

(d) **The Application Owner** assists the CISO and instruct the relevant technical team in ensuring timely closure of vulnerabilities.

(e) **The SeMT/CeG Team** coordinates with all stakeholders to ensure timely communication and closure of vulnerabilities, as well as maintaining the **State Level Application Information Repository**.

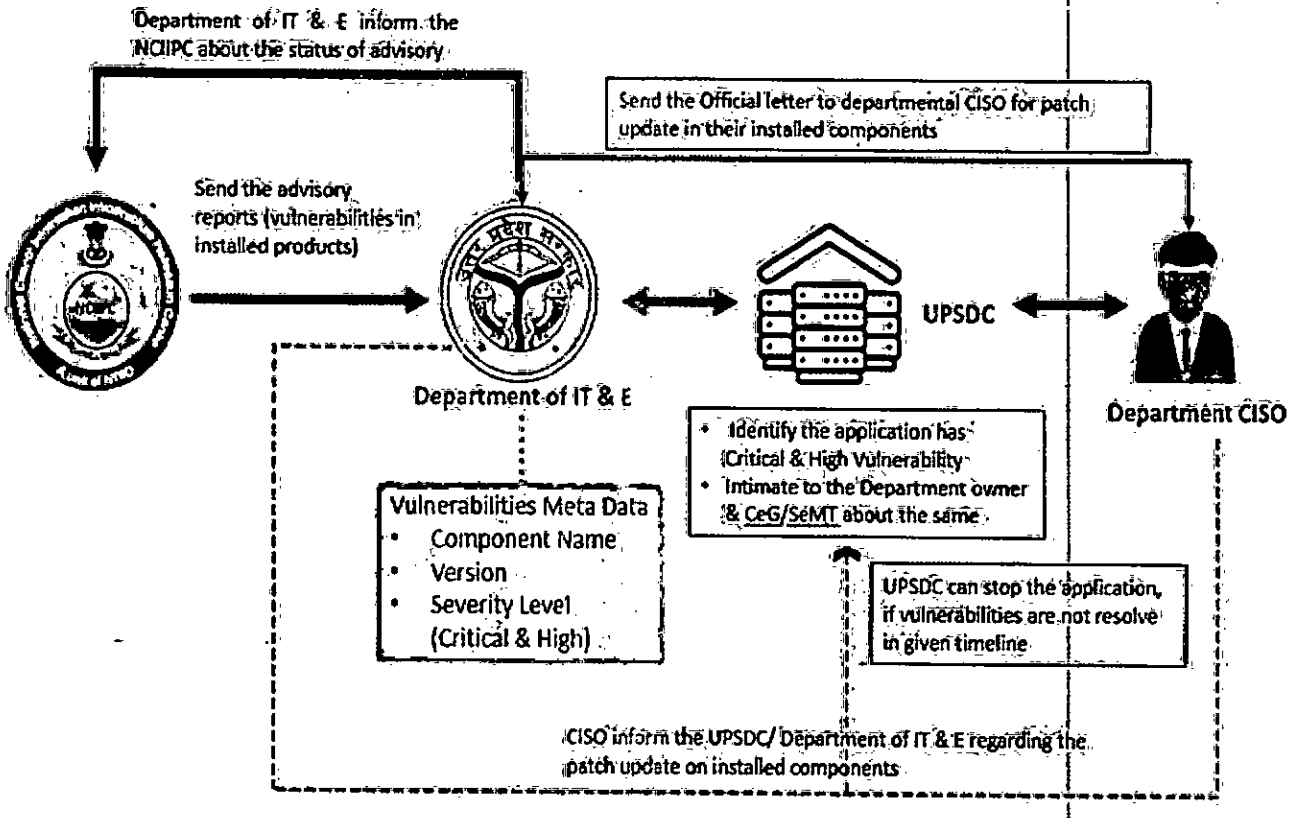
(f) **The UPSDC Team** sends reminders, deactivates applications if vulnerabilities are not resolved, and updates the **State Level Application Information Repository** for applications hosted in UPSDC.

(g) **The Technical Team** of the concerned department is responsible for closing vulnerabilities within the given timeframe and ensuring that no such vulnerabilities exist in the hosted application.

7. It is also recommended to create, update and maintain a **State Level Application Information Repository** for all hosted applications and their installed third-party components along with their versions across the State Line Departments. The repository should tentatively include the following fields to be maintained:

- Name of Department
- Application Name
- Hosting Place (SDC/ or other Cloud Platform (Name of the Cloud Platform)
- Url of the Application
- Nature of Application (Critical/ Non-Critical)
- Installed Components Details
- Name, Version, Company name, any other details
- CISO
- Deputy CIS
- Owner of the Application

8. Process Flow



SoP for Resolving Vulnerabilities Identified in Uttar Pradesh Websites/ Web Applications by NCIIPC

1. Introduction

NCIIPC conducts regular audits of State Critical Information Infrastructures (CII) to safeguard them against cyber attacks. As part of this advisory, NCIIPC provides information on vulnerable websites or web applications for immediate resolution. Taking swift action is advised to address the identified vulnerabilities in the impacted website or web application.

2. Abbreviation

S. No.	Abbreviation	Description
1	NCIIPC	National Critical Information Infrastructure Protection Centre
2	CISO	Chief Information Security Officer
3	SeMT	State e-Governance Mission Team
4	CeG	Centre for e-Governance
5	UPSDC	Uttar Pradesh State Data Center
6	SoP	Standard Operating Procedure

3. Traffic Light Protocol (TLP)

The advisory provided by NCIIPC includes a Traffic Light Protocol (TLP), which specifies the intended audience for sharing. TLP promotes enhanced information sharing by categorizing information into different levels to ensure it is shared appropriately. It utilizes four colors to denote expected sharing boundaries for the recipients. Below are the definitions of TLP levels:

TLP: Red	Not for disclosure, restricted to participants only.
TLP: Amber+Strict	Limited disclosure, restricted to participants' organization.
TLP: Amber	Limited disclosure, restricted to participants' organization and its clients
TLP: Green	Limited disclosure, restricted to the community.
TLP: Clear	Disclosure is not limited.

4. Key Stakeholders

(a) NCIIPC

(b) State CISO

(c) Department CISO

(d) Deputy CISO

(e) SeMT/ CeG Team

(f) UPSDC Team

(g) Application owner of hosted application

(h) Technical Team of respective Application

5. **Step for Vulnerability Resolution in the Website/ Web application**

(a) The State CISO sends the vulnerable website/ web application information received from NCIIPC to the SeMT team via email for prompt action.

(b) The SeMT team notifies the respective Department CISO, Deputy CISO, and UPSDC Manager about the vulnerable website/ web application. They share details such as:

- ❖ Name of the Department
- ❖ Name of the Website/ Web Application
- ❖ URL of the Website/ Web Application
- ❖ Vulnerability Details

(c) Vulnerabilities disclosed must be fixed **within two weeks** from the reporting date to the respective department.

(d) The CISO, with the help of the Deputy CISO and application owner, instructs the relevant team to fix the vulnerability within the set timeline and updates the concerned stakeholders (e.g., State CISO, SeMT/CeG Team and UPSDC Manager/UPSDC team).

(e) It is also recommended to conduct full audit of the application after resolving the vulnerability.

(f) **If the vulnerable website or web application is hosted in UPSDC**, the **UPSDC Manager deactivates it if the vulnerabilities are not resolved within the given timeline**. Three reminders are sent by the UPSDC team to the application owner and other stakeholders: two reminders in the first week and one reminder in the second week.

(g) The SeMT team coordinates and updates the NCIIPC about the status of vulnerability closure.

6. **Role & Responsibility of Stakeholder**

(a) **The State CISO** oversees and monitors the entire process of vulnerability closure.

(b) **The Department CISO** ensures that vulnerabilities are addressed within the

specified timeframe.

(c) **The Deputy CISO** technically assists CISO in vulnerability closure.

(d) **The Application Owner** assists the CISO and instruct the relevant technical team in ensuring timely closure of vulnerabilities.

(e) **The SeMT/CeG Team** coordinates with all stakeholders to ensure timely communication and closure of vulnerabilities, as well as maintaining the **State Level Application Information Repository**.

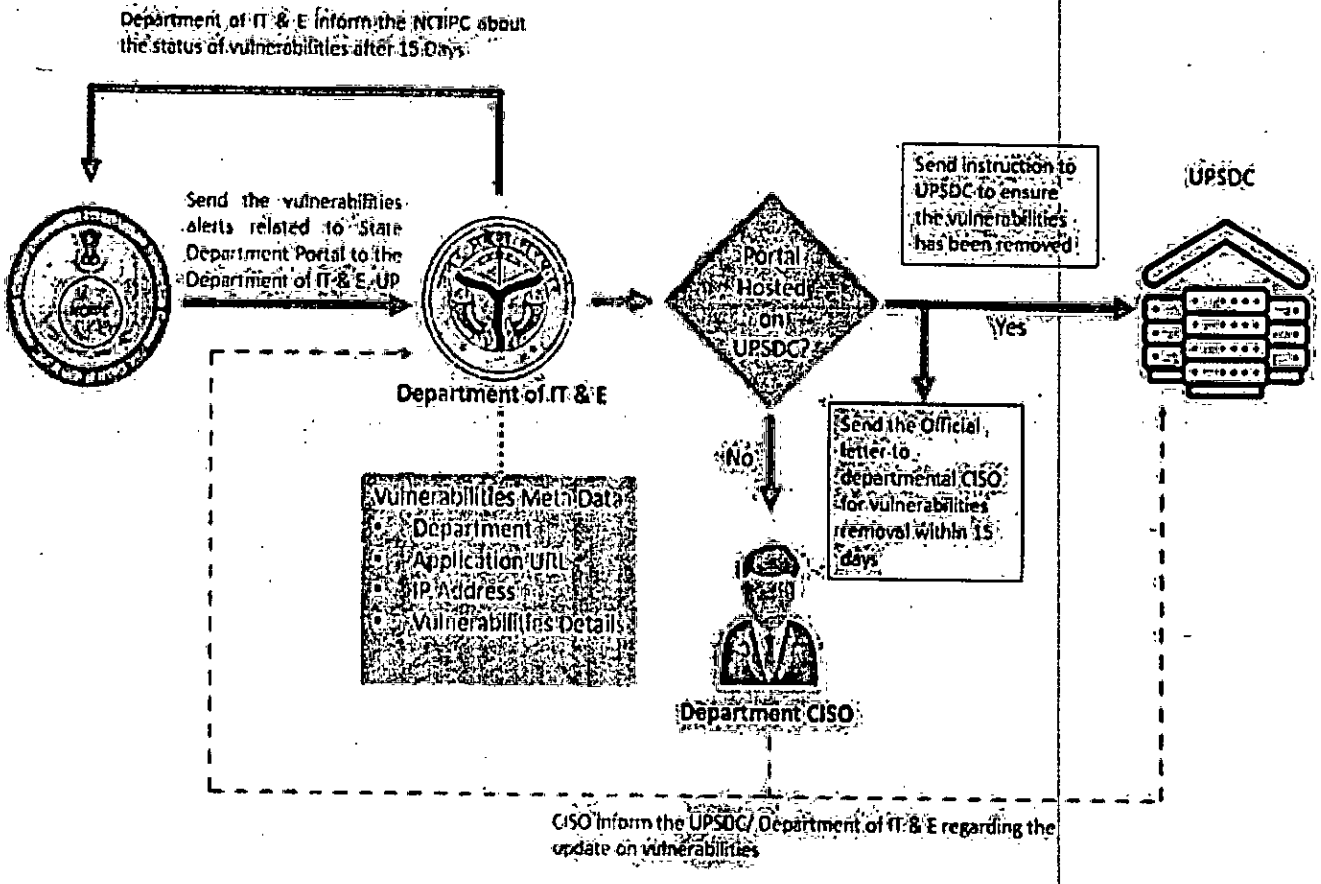
(f) **The UPSDC Team** sends reminders, deactivates applications if vulnerabilities are not resolved, and updates the **State Level Application Information Repository** for applications hosted in UPSDC.

(g) **The Technical Team** of the concerned department is responsible for closing vulnerabilities within the given timeframe and ensuring that no such vulnerabilities exist in the hosted application.

7. It is also recommended to create, update and maintain a **State Level Application Information Repository** for all hosted applications and their installed third-party components along with their versions across the State Line Departments. The repository should tentatively include the following fields to be maintained:

- Name of Department
- Application Name
- Hosting Place (SDC/ or other Cloud Platform (Specify the Name of the Cloud Platform)
- Url of the Application
- Nature of Application (Critical/ Non-Critical)
- Installed Components Details
- Name, Version, Company name, any other details
- CISO
- Deputy CISO
- Owner of the Application

8. Process Flow



SoP for Implementing Cyber Security Advisory - Indicators of Compromise (IOCs) by NCIIPC

1. Introduction

An Indicator of Compromise (IoC) is a piece of information that indicates a potential security breach or cyberattack. NCIIPC shares malicious URLs & IPs under this advisory. It is recommended to immediately blocks these URLs/ IPs in their Firewalls/ other security systems to protect Critical Information Infrastructure of the State.

2. Abbreviation

S. No.	Abbreviation	Description
1	NCIIPC	National Critical Information Infrastructure Protection Centre
2	CISO	Chief Information Security Officer
3	SeMT	State e-Governance Mission Team
4	CeG	Centre for e-Governance
5	UPSDC	Uttar Pradesh State Data Center
6	SoP	Standard Operating Procedure

3. Traffic Light Protocol (TLP)

The advisory provided by NCIIPC includes a Traffic Light Protocol (TLP), which specifies the intended audience for sharing. TLP promotes enhanced information sharing by categorizing information into different levels to ensure it is shared appropriately. It utilizes four colors to denote expected sharing boundaries for the recipients. Below are the definitions of TLP levels:

TLP: Red	Not for disclosure, restricted to participants only.
TLP: Amber+Strict	Limited disclosure, restricted to participants' organization.
TLP: Amber	Limited disclosure, restricted to participants' organization and its clients
TLP: Green	Limited disclosure, restricted to the community.
TLP: Clear	Disclosure is not limited.

4. Key Stakeholders

(a) NCIIPC

(b) State CISO

(c) Department CISO

(d) Deputy CISO

(e) SeMT/ CeG Team

(f) UPSDC Team

(g) Application owner of hosted application

(h) Technical Team of respective Application

5. **Step for Implementation of Cyber Security Advisory - IOCs**

1) The State CISO sends the IoC advisory received from NCIIPC to the SeMT team via email for prompt action.
2) The SeMT team informs the respective Department CISO, Deputy CISO, and UPSDC Manager about the cyber security advisory and recommends updating it in their firewall or wherever applicable. They share details such as
   - ❖ IoC – IPs (Internet Protocol)
   - ❖ IoC – URLs (Uniform Resource Locator)
3) IoCs should be implemented within 48 hours from the reporting date. Both the UPSDC Manager/UPSDC team and Department CISO/Deputy CISO should acknowledge, implement, and share their status via email to the concerned stakeholders (State CISO, SeMT/CeG, Application Owner).
4) The SeMT team coordinates and updates the NCIIPC about the status of the implementation.

6. **Role & Responsibility of Stakeholder**

(a) **The State CISO** is responsible for overseeing and monitoring the overall process of implementing IoCs.

(b) **The Department CISO** ensures that IoCs advisories are implemented within the specified timeline.

(c) **The Deputy CISO** technically assists CISO in implementing cyber security-related advisories.

(d) **The Application Owner** assists the CISO in ensuring the implementation of IoCs advisories within the given timeline.

(e) **The SeMT/CeG Team** coordinates with all stakeholders to ensure timely dissemination of information and implementation of IoCs advisories.

(f) **The UPSDC Team** ensures the implementation of IoCs advisories within the given timeline.

(g) **The Technical Team** of the concerned department is also responsible for implementing IoCs advisories under the supervision of the CISO & application owner.

7. Process Flow