लेक्चर संख्या	संचालनालय स्तर पर अधिकारियों के लिए "CEDCLPCSMS100 - साइबर सुरक्षा प्रबंधन और अनुपालन" प्रशिक्षण पाठ्यक्रम	अवधि/ कुल घंटे
	विषय-वस्तु	
विषय	**साइबर स्पेस, साइबर सुरक्षा, साइबर अपराध एवं साइबर क़ानून**	
	परिचय : • साइबर स्पेस एवं शिष्टाचार • साइबर सुरक्षा अवधारणा, परिभाषा (आईटी अधिनियम के अनुसार) और सिद्धांतों को समझें • साइबर सुरक्षा का महत्व एवं आवश्यकता **साइबर कानून के बारे में संक्षिप्त जानकारी-** • सूचना प्रोद्योगिकी अधिनियम, 2000 पर परिचय एवं महत्त्वपूर्ण प्रावधान • डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 पर परिचय एवं महत्त्वपूर्ण प्रावधान **साइबर अपराध और इसकी रोकथाम:** • साइबर अपराध का परिचय एवं श्रेणी • सूचना प्रोद्योगिकी अधिनियम, 2000 में परिभाषित अपराध • साइबर अपराध के प्रकार: • महिलाओं के खिलाफ ऑनलाइन साइबर अपराध और प्रतिरूपण घोटाले • कार्यस्थल पर साइबर अपराध	**02 घंटा**

	ऑनलाइन वित्तीय धोखाधडी और इसकी रोकथाम • विभिन्न ऑनलाइन गतिविधियों से जुड़ा साइबर जोखिम और उससे सुरक्षा उपाय। • कियोस्क बैंकिंग, एटीएम एवं आधार कार्ड आधारित फ्रॉड • पहचान चोरी एवं दस्तावेज का दुरुपयोग कर अवैध लोन, ओटीपी एवं अन्य SMS आधारित फ्रॉड, अज्ञात / असत्यापित मोबाइल ऐप फ्रॉड, लोन शेयर मार्केट, ई केवाईसी, रीमोट एक्सेस, मोबाईल रिचार्ज शॉप फ्रॉड इत्यादि, • मनी म्यूल एकाउंट्स: नये / फ़र्ज़ी खाते खोलने एवं बैंक खातों का ऑनलाइन फ्रॉड में दुरुपयोग • फिशिंग लिंक, विशिंग कॉल, एटीएम कार्ड स्किमिंग, ऑनलाइन सेलिंग प्लेटफॉर्म का उपयोग कर धोखाधड़ी, लॉटरी स्कैम, फर्जी इनवेस्टमेंट स्कैम, ऑनलाइन जॉब फ्रॉड, क्यूआर कोड स्केन फ्रॉड, सर्च इंजन फ्रॉड, सोशल मीडिया के माध्यम से प्रतिरुपण • ई-बैंकिंग सेवा (आरटीजीएस/ आईएमपीएस / एनईएफटी) आधारित धोखाधड़ी, ई सिम फ्रॉड, सिम स्वैप / सिम क्लोनिंग, एसएमएस / ईमेल / इंस्टेंट मैसेजिंग / कॉल स्कैम, ऑनलाइन शॉपिंग फ्रॉड **शिकायत दर्ज करने हेतु प्रक्रिया** •साइबर अपराध सम्बन्धी शिकायत, मध्य प्रदेश साइबर सेल, ऑनलाइन साइबर क्राइम एवं बैंक फ्रॉड की शिकायत, यू पी आई संबंधी शिकायत •आरबीआई बैंक लोकपाल को शिकायत, बैंक में शिकायत, हेल्पलाइन नंबर •सोशल मीडिया एवं ऑनलाइन सेवा प्रदाताओं को शिकायत •साइबर अपराध की शिकायत के लिए आवश्यक दस्तावेज क्या हैं? •न्याय निर्णायक अधिकारी	
विषय	**ई-गवर्नेंस एवं शासकीय कंप्यूटर संसाधनों से संबंधित नीति, नियम एवं सुरक्षा क़ान**	**02 घंटा**
	ई -प्रोक्योरमेंट और ई-टेंडरिंग (E-Procurement and E-tendering) –I: **सबंधित साइबर खतरे, सुरक्षा उपाय, आई टी नियम-निर्देश एवं केस अध्ययन**	
	इलेक्ट्रॉनिक रिकॉर्ड एवं डिजिटल सिग्नेचर सर्टिफिकेट: • **इलेक्ट्रॉनिक रिकॉर्ड एवं इलेक्ट्रॉनिक रिकॉर्ड की प्रामाणिकता** • डिजिटल सिग्नेचर क्या है, कौन जारी करता है तथा कितने प्रकार के होते है • क़ानूनी वैद्यता एवं प्रावधान • डिजिटल हस्ताक्षर का उपयोग कर इलेक्ट्रॉनिक रिकॉर्ड का प्रमाणीकरण • डिजिटल हस्ताक्षर: तकनीकी एवं कानूनी मुद्दे	
	शासकीय कंप्यूटर एवं कंप्यूटर संसाधनों से संबंधित कानून • आईटी अधिनियम 2000 के तहत संरक्षित प्रणाली एवं महत्व • कंप्यूटर एवं कंप्यूटर संसाधनों से संबंधित कानून • मध्य प्रदेश ईमेल नीति 2014 का अवलोकन	
	साइबर सुरक्षा: कार्यालय में साइबर सुरक्षा फ्रेमवर्क स्थापित करना	

<table>
<tr><td></td><td colspan="2">नियम एवं दिशा-निर्देश
● सरकारी अधिकारियों के लिए साइबर सुरक्षा गाइडलाइन
● शासकीय कंप्यूटर एवं कंप्यूटर संसाधनों के प्रति उपयोगकर्ता कर्मचारी की ज़िम्मेदारी
इलेक्ट्रॉनिक रिकॉर्ड और सूचना की गोपनीयता और सुरक्षा</td><td></td></tr>
<tr><td>विषय</td><td colspan="2">जांच करने में जांच अधिकारी/प्रस्तुतकर्ता अधिकारी की भूमिका</td><td rowspan="2">02 घंटा</td></tr>
<tr><td></td><td colspan="2">साइबर अपराध जांच/ अन्वेषण: हैंडलिंग और घटना प्रतिक्रिया
1. साइबर अपराध की हैंडलिंग और रिपोर्टिंग
• साइबर अपराध की प्रकृति को समझें
• साइबर अपराध बनाम पारंपरिक अपराध
• साइबर अपराध जांच प्रक्रिया एवं मानक संचालन प्रक्रिया
• साइबर अपराध की रिपोर्टिंग
• एक अच्छी शिकायत को कैसे तैयार करें
• आंतरिक जांच से संबंधित महत्त्वपूर्ण तथ्य
• इलेक्ट्रॉनिक साक्ष्य और उपकरणों की हैंडिलिंग एवं सुरक्षा प्रक्रिया
2. साइबर अपराध जांच से संबंधित महत्वपूर्ण तथ्य
• साइबर फोरेंसिक
• चैन ऑफ कस्टडी
• हैशिंग और हैश मूल्य का महत्व
• फैराडे बैग (Faraday Bag)
• डिजिटल हस्ताक्षर
3. केस स्टडी</td></tr>
<tr><td>विषय</td><td colspan="2">साइबर सुरक्षा प्रबंधन: कार्यान्वयन, अनुपालन और मूल्यांकन</td><td>10 घंटे</td></tr>
<tr><td></td><td colspan="2">परिचय- साइबर सुरक्षा प्रबंधन समाधान: कार्यान्वयन, अनुपालन और मूल्यांकन
सुरक्षा नियंत्रण (सुरक्षा कंट्रोल)
1. NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS द्वारा "SAFETY AND SECURITY OF CHILDREN IN SCHOOLS" में निर्धारित साइबर सुरक्षा नियंत्रण (Section I)
Section-I Cyber Safety
<table>
<tr><th>S.No.</th><th>Statements</th></tr>
<tr><td>1</td><td>Is access to computer rooms and use of electronic and technological devices by students supervised by teachers?</td></tr>
<tr><td>2</td><td>Are Social Networking sites blocked in the school computers?</td></tr>
<tr><td>3</td><td>Are students regularly educated on safe usage of technology and how to be responsible digital citizen –sensible use of mobiles, sms, mms, internet, mail or net chats, effect of plagiarism and how to avoid risky behavior?</td></tr>
<tr><td>4</td><td>Are students educated to understand their responsibilities, the consequences under the laws on cyber misuse, bullying, harassment etc.?</td></tr>
</table></td><td></td></tr>
</table>

5	Are School Authority and children oriented on procedures to be followed and steps prescribed within the legal frame work in the event of cyber abuse or crime – legal recourse and information about Cyber
6	Are cyber-crimes handled with sensitivity and confidentiality?
7	Whether the school have a document that defines procedures and policies that the school implements to safeguard against any online safety incident?
8	Whether the school have a special committee that implements the provisions under the guidelines regarding cyber safety?
9	Whether the school have any draft policy regarding actions to be taken against an accused (Students, teachers or other staff members) of cyber-crime?
10	Whether or not the school have any monitoring committee to track any kind of cyber- attack on children when at school?
11	Whether or not the school provides education regarding cyber-crimes through various mediums to educate the child about what cyber-crimes are and what are the do's and don'ts that a child must keep in mind to ensure his/her safety and further are children educated to keep their personal data and information secure to minimize the risks of cyber-crime?
12	Whether or not the school have a special redressal cell for a child victim of any kind of cyber- crime / Whether or not the school have proper information as to which authority's cybercrime can be reported? Are School Authority and children oriented on procedures to be followed and steps prescribed within the legal framework in the event of cyber abuse or crime – legal recourse and information about Cyber Crime Department in the Police?
13	Whether or not the school ensures supervision on children when they attend computer labs classes or any other classroom where they can become a victim of cyber-crime?
14	Whether or not the staff of the school are well informed/educated on e-safety/cyber-safety of children?
15	Does the school have any drafted policy on misuse of technology/equipment by pupils and staff?
16	Does the school have any policy on monitoring the usage of camera's including webcams, the use of video conferencing equipment, mobile phones etc. by the staff or children to ensure safety of children.
2. Computer Emergency Reponses Team- Indian (Ministry….) द्वारा निर्धारित Guidelines on Information Security Practices for Government Entities " साइबर सुरक्षा नियंत्रण (Section II)		
Section II - Guidelines on Information Security Practices for Government Entities		
General Security Controls		
A non-disclosure agreement should be signed along with access request, by the individual employees of third-party entering Institution's facilities or accessing their information assets.		

	Agreements are up to date and remain effective over time.	
	The Organization Endpoints is suitably protected from data exfiltration through Security Solutions like DLP etc.	
	Data must not be shared with outsiders without explicit & case specific approval of authority	
	Third party/Vendor has a mechanism in place to ensure that the employees return the assets containing Institution data after role change or completion/ termination of the project or company.	
	Periodic security awareness training should be conducted for Institution by authority.	
	Ensure Compliance of Vulnerability Assessment / Penetration Testing observations for assets managed by Vendor resources.	
	Remote access is disabled on Institution systems other than specific approval of authority at specific time period and date	
	Access control is properly defined and access to Institution information systems is strictly on Need-to- Know / Need-to-have basis.	
	Institution is using licensed version of Antivirus Software and updated with latest updates to provide protection for online transaction	
	CCTV surveillance system (CCTV footage is recorded and stored for 90 days) & Proper system is in place for continuous monitoring of CCTV footage	
	Adequate controls of printouts taken from the system are in place and log is maintained for printout taken and kept securely	
	Institution follow the proper system of training to employees who access Institution information system for the job entrusted to them	
	Employees ensures data confidentiality as per the provision & policies of Institution	
	Physical and logical security of system is regulated and allowed to authorized person only	
	The password policy (Strong passwords are stipulated) of the vendor prohibits its sharing and there is regular training in this regard	
	There is a well-defined process for removing the user account and access rights at the time of employee leaving the organization	
	There is a periodic review/ verification of user access profile by the system administrator (vendor)	
	Institution has a process in place for reporting security breaches to the management/authority	
	The Institution/employees should not use Virtual Private Network (VPN) on PC/Laptop without specific approval of authority/management	
	Admin privileges and access to USB/CD are restricted on Desktop/Laptop of Institution	
	Institution should not store sensitive information like Aadhar number & Fingerprints of employees or other personnel, or if required for business continuity then prepare and implement reasonable security practice and procedure and policy as per applicable laws like Information Technology Act, 2000 and Digital Data Personal Act, 2023	
	NETWORK & INFRASTRUCTURE SECURITY	
	Change all default credentials & configuration at the time of first installation	

	Bring Your Own Device (BYOD) should be restricted and no unknown devices should be allowed in the network without authorization by the Network Administrator.	
	Ensure that there is a segmentation of Wi-Fi users and/or devices on the basis of SSID./if not add device binding	
	Ensure that customized access policies are applied per SSID as per the requirements.	
	Ensure to change default configuration & credentials of Wireless access point.	
	Institution must ensure that all available measures are applied on Access Points (APs) or WLAN switches to secure them from unauthorized access.	
	Use of personal devices must be authorized by concerned Network Administrator of the Institution and in accordance with cyber security policy.	
	Unauthorized access, physical damage, and tampering to IT systems should be prevented by implementing physical security	
	The Institution must ensure that default credentials of network devices and information systems such as usernames, passwords, and tokens are changed prior to their deployment or first use	
	All devices at User level should use USER account and use of Administrator account should be restricted to Network/System Administrators only.	
	INTERNET SECURITY	
	Use Private Browsing/Incognito Mode in your browser while accessing Government applications/services, email services or banking/payment related services or any other important application/services.	
	Directly click on the link while accessing sites where user login is required, always type the site's domain name/URL.	
	Use the latest version of the internet browser	
	Ensure that the browser is updated with the latest updates/patches?	
	Don't store any usernames and passwords on the internet browser.	
	Don't store any payment related information on the internet browser.	
	Don't use any 3rd party anonymization services (ex: Nord VPN, Express VPN, Tor, Proxies etc.).	
	Don't use any 3rd party toolbars (ex: download manager, weather tool bar, ask me tool bar etc.) in your internet browser.	
	Don't use your official systems for installing or playing any Games?	
	Do not click directly on any shortened URLs (ex: tinyurl.com/ab534/) which may lead to a phishing/malware webpage, which could compromise your device.	
	Change passwords at least once in 30 days.	
	Use Multi-Factor Authentication, wherever available.	
	How to enable, disable, view or delete Internet cookies and browser history?	
	How to manage your website privacy and security.	
	How to manage auto-password and auto-fill data.	
	How to use a secure Wi-Fi network.	
	How to use secure URL site (using https secure URL only).	
	How to identify real and fake websites.	
	DESKTOP/LAPTOP/PRINTER SECURITY	
	Whether Standard User (non-administrator) account is set for the user for accessing the computer/laptops for regular work?	
	Whether BIOS Password is configured for booting?	
	Whether OS update is set to auto-update from a trusted source.	

	Whether Government offered Antivirus is Installed on official desktops/laptops and configured for update?	
	Whether it has been ensured that Applications/software's used are part of authorized list?	
	Whether it has been ensured that pirated or software that are not part of authorized list of applications/software are uninstalled?	
	Whether security of password enforced as per the guidelines?	
	Whether it is ensured to allow only authorized USB storage devices, external storage devices?	
	Whether printers are configured as per the guidelines?	
	Never allow admin account to use by other/guest	
	Ensure that you always lock/log off from the desktop when not in use	
	Shutdown the desktop before leaving the office.	
	REMOVABLE MEDIA SECURITY	
	Only use authorized and approved removable media devices provided by the organization.	
	Instruct employees to label all removable media with their name, date, and purpose.	
	Inspect removable media for any signs of physical damage or tampering before use.	
	Store removable media in a secure and designated location when not in use.	
	Implement physical security measures, such as locked cabinets or safes, for media storage.	
	Do not leave removable media unattended or in easily accessible areas	
	Perform a low format of the removable media before the first-time usage.	
	Avoid copying or storing personal or sensitive data on removable media without proper authorization.	
	Obtain necessary authorization before using removable media for any purpose.	
	Prohibit the use of personal or unauthorized removable media within the organization.	
	Scan the removable media with Antivirus software before accessing it	
	Avoid using removable media on public or untrusted computers to minimize the risk of malware or unauthorized access.	
	Always protect your documents with strong password.	
	Never share removable media with unauthorized individuals or organizations.	
	EMAIL SECURITY	
	Password Protection- as per password policy	
	Avoid using personal information in passwords.	
	Update passwords once in a month	
	Regularly review the past login activities by clicking on the "login history" tab.	
	Use a Two factor authentication	
	Do not click on suspicious links.	
	Never use any unauthorized/external email services for official communication.	
	Never open sensitive documents in public networks	
	Verify sender's email address before download attachment	
	Enable encryption in file transfer through email	
	Section III	

	मोबाइल सुरक्षा: • फोन में कितने प्रकार के पॉसवर्ड दाल सकते है तथा कैसे सेट करें। • फ़ोन में एप्लिकेशन अनुमति कैसे प्रबंधित करें • रिमोट एक्सेस एप्लिकेशन सुरक्षा उपाय • डाउनलोड करने से पहले कैसे जांचें कि कौन सा एप्लिकेशन फोन में कौन सी अनुमति का उपयोग करेगा? • विज्ञापन आईडी कैसे बदलें और इसके क्या फायदे हैं • आपको मोबाइल फ़ोन में कोई भी अवांछित एप्लिकेशन क्यों डाउनलोड नहीं करना चाहिए • मोबाइल से थर्ड पार्टी एप्लिकेशन डेटा एक्सेस कैसे हटाएं • Google, सोशल मीडिया अकाउंट में 2 फैक्टर वेरिफिकेशन कैसे सेट अप करें। • फोन में एप्लिकेशन की अनुमति कैसे प्रबंधित करें डाउनलोड से पहले यह कैसे जांचें कि कौन सा एप्लिकेशन • फोन में किस अनुमति का उपयोग करेगा? • आपके नाम पर कितनी सिम चल रही है कैसे पता करें। **सोशल मीडिया अकाउंट सुरक्षा:-** • जीमेल पर 2 स्टेप वेरिफिकेशन कैसे एक्टिवेट करें • सोशल मीडिया अकाउंट को कैसे सुरक्षित करें • विवरण: खाता गोपनीयता, स्थिति गोपनीयता, कहानी गोपनीयता, टिप्पणी करना, 2 चरण सत्यापन, संदेश नियंत्रण, अभिभावकीय नियंत्रण आदि। • सोशल मीडिया पर अकाउंट और फोटो कैसे डिलीट करें? • इंस्टाग्राम अकाउंट को कैसे डीएक्टिवेट और डिलीट करें? • फेसबुक अकाउंट को डीएक्टिवेट और डिलीट कैसे करें? • फेसबुक पर अकाउंट और फोटो की रिपोर्ट कैसे करें? • इंस्टाग्राम पर अकाउंट और फोटो की रिपोर्ट कैसे करें? • व्हाट्स ऐप नंबर बदलें और अकाउंट डिलीट करें? **ऑनलाइन सुरक्षित बैंकिंग:-** • ई-कॉमर्स वेबसाइट और पेमेंट गेटवे का सुरक्षित उपयोग • बैंक खाता सुरक्षा (इंटरनेट बैंकिंग, एनईएफटी, आईएमपीएस और अन्य लेनदेन) • UPI और AePS भुगतान सुरक्षा और शिकायत/रिपोर्टिंग प्रक्रिया • रिक्वेस्ट मनी यूपीआई घोटाला • वैध निगमन या कंपनी का सत्यापन कैसे करें • ऑनलाइन बिल भुगतान (जैसे ऑनलाइन रिचार्ज, बिजली, पानी और इंटरनेट बिल, ऑनलाइन फूड ऑर्डरिंग प्लेटफॉर्म, होटल बुकिंग, आरक्षण, यात्रा संबंधी सेवाएं) सुरक्षा उपाय • सुरक्षित बैंकिंग लेनदेन (फंड ट्रांसफर करें, ऋण भुगतान करें, वित्त प्रबंधन करें) • डिजिटल वॉलेट सुरक्षा एवं संरक्षा • डेबिट और क्रेडिट कार्ड सुरक्षा **अन्य सुरक्षा उपाय:-**	

	• अपने खोए/चोरी हुए फ़ोन को कैसे ब्लॉक करें? • अपने मोबाइल कनेक्शन कैसे जानें • भारतीय नंबर से अंतर्राष्ट्रीय इनकमिंग कॉल की रिपोर्ट कैसे करें • आधार प्रमाणीकरण इतिहास कैसे जांचें • बायोमेट्रिक्स को लॉक/अनलॉक कैसे करें • मास्क्ड आधार कार्ड कैसे डाउनलोड करें	