



म.प्र. राज्य मुक्त स्कूल शिक्षा बोर्ड, भोपाल

स्कूल शिक्षा विभाग मध्यप्रदेश शासन
शिवाजी नगर, भोपाल – 462011

Phone : 0755-2552106
Web Site : www.mpsos.nic.in
E-Mail : mpsos2022@gmail.com

पाठ्यक्रम

सर्टिफाइड साइबर सिक्योरिटी मैनेजर (Certified Cyber Security Manager - CCSM) (नियम, परीक्षा, योजना, अंकन, योजना एवं पाठ्यक्रम)

सत्र: 2025-26

1. पाठ्यक्रम का परिचय एवं उद्देश्य:

वर्तमान परिदृश्य में शासकीय एवं निजी कार्यालयों में तथा ऑनलाइन एवं परंपरागत व्यावसायों में कंप्यूटर संसाधनों तथा डिजिटल तकनीकी का उपयोग हो रहा है। जैसा की लगातार दैनिक समाचारों व घटनाओं से यह स्पष्ट हो रहा है कि कंप्यूटर संसाधनों पर साइबर अटैक जैसे रेंसमवेयर, हैकिंग, डाटा चोरी इत्यादि के साथ साथ साइबर फ्रॉड व मानवीय लापरवाही एवं तकनीकी ज्ञान की कमी होने के कारण संस्थानों को बड़े पैमाने पर वित्तीय क्षति का सामना करना पड़ता है। इससे व्यवसाय को तकनीकी जोखिम का सामना करना पड़ता है और इसका प्रभाव व्यवसाय के साथ साथ लोगों की निजी जिंदगी पर भी पड़ता है।

उक्त साइबर खतरों से निपटने के लिए संस्थानों में उपयोग होने वाले कंप्यूटर संसाधन, डाटा व नेटवर्क के सुरक्षित उपयोग एवं प्रबंधन के लिए मानक तकनीकी सुरक्षा उपाय और संसाधन जैसे फायरवाल, एंटीवाइरस इत्यादि का उपयोग करना आवश्यक हो गया है। संस्था में साइबर सुरक्षा ऑफिसर की भूमिका महत्वपूर्ण है जो मुख्य रूप से तकनीकी संसाधनों व सुरक्षा क्रियान्वयन व आंतरिक सुरक्षा ऑडिट के लिए जिम्मेदार हो। इससे साइबर जोखिम व साइबर अपराधों की कार्यस्थल पर रोकथाम की जा सकती है।

“सर्टिफाइड साइबर सिक्योरिटी मैनेजर” (Certified Cyber Security Manager- CCSM) पाठ्यक्रम विशेष रूप से संस्थानों में मानक साइबर सुरक्षा कंट्रोल एवं संसाधनों को क्रियान्वित व साइबर सुरक्षा प्रबंधन करने के उद्देश से तैयार किया गया है। जिसमें अभियार्थियों, को साइबर सुरक्षा ऑफिसर के रूप में तैयार किया जाता है। साइबर सुरक्षा ऑफिसर संस्था में सूचना व कंप्यूटर संसाधनों की सुरक्षा प्रबंधन के लिए जिम्मेदार होता है।

इस पाठ्यक्रम का उद्देश्य प्रतिभागियों को साइबर सुरक्षा के मूल सिद्धांतों, नेटवर्क सुरक्षा, डेटा संरक्षण, साइबर कानूनों, सुरक्षा ऑडिट व अनुपालन और साइबर सुरक्षा प्रबंधन की व्यावहारिक समझ प्रदान करना है। पाठ्यक्रम के माध्यम से अभियार्थी न केवल तकनीकी ज्ञान अर्जित करेंगे, बल्कि वे सुरक्षा नीतियों को बनाने, टीमों का नेतृत्व करने और संगठनों में एक मजबूत साइबर सुरक्षा ढांचा स्थापित करने में सक्षम बनेंगे।

2. रोजगार एवं स्वरोजगार के क्षेत्र

“सर्टिफाइड साइबर सिक्योरिटी मैनेजर” (Certified Cyber Security Manager- CCSM) पाठ्यक्रम प्रतिभागियों को न केवल तकनीकी विशेषज्ञता प्रदान करता है, बल्कि उन्हें आधुनिक डिजिटल दुनिया में रोजगार और स्वरोजगार के बहुआयामी अवसरों के लिए भी तैयार करता है। इस कोर्स को सफलतापूर्वक पूरा करने के बाद अभियार्थी विभिन्न सरकारी एवं निजी संगठनों, बैंकिंग एवं वित्तीय संस्थानों, आईटी कंपनियों, शिक्षा संस्थानों, हेल्थकेयर, ई-कॉमर्स, और रक्षा क्षेत्र में साइबर सुरक्षा विशेषज्ञ, सूचना सुरक्षा अधिकारी (Information Security Officer), सूचना सुरक्षा सहायक (Information Security Assistant), नेटवर्क सुरक्षा विश्लेषक, आईटी ऑडिटर, या सिस्टम सिक्योरिटी मैनेजर के रूप में कार्य कर सकते हैं।

मध्य प्रदेश सरकार ने साइबर खतरों से निपटने, डिजिटल परिसंपत्तियों की सुरक्षा सुनिश्चित करने और समग्र साइबर सुरक्षा ढांचे को मजबूत करने के उद्देश्य से MP-CERT (Madhya Pradesh – Computer Emergency Response Team) का गठन किया है। इसके तहत राज्य के प्रत्येक विभाग में Certified Information Security Officer (CISO) की नियुक्ति की गई है, जो विभागीय डेटा, नेटवर्क, और डिजिटल प्रणालियों की सुरक्षा सुनिश्चित करने के लिए जिम्मेदार हैं। यह कदम न केवल साइबर हमलों से बचाव के लिए आवश्यक है, बल्कि यह साइबर सुरक्षा पेशेवरों के लिए रोजगार के नए अवसर भी प्रस्तुत करता है।

इस प्रकार, " सर्टिफाइड साइबर सिक्योरिटी मैनेजर (Certified Cyber Security Manager - CCSM) " जैसे पाठ्यक्रम अब केवल निजी कंपनियों के लिए ही नहीं, बल्कि सरकारी क्षेत्रों में भी करियर की मजबूत संभावनाएं प्रदान करते हैं।

साथ ही, स्वरोजगार की दिशा में इच्छुक प्रतिभागी फ्रीलांस साइबर सिक्योरिटी कंसल्टेंट/ ऑडिटर या साइबर सुरक्षा प्रशिक्षक/ट्रेनर के रूप में अपनी सेवाएं प्रदान कर सकते हैं। डिजिटल सेवाओं की बढ़ती मांग के कारण वे अपने स्टार्टअप या साइबर सिक्योरिटी फर्म की शुरुआत भी कर सकते हैं, जो विशेष रूप से व्यवसायों, स्कूलों, और संस्थाओं को साइबर सुरक्षा समाधान प्रदान करें।

3. पाठ्यक्रम विवरण:

पाठ्यक्रम शीर्षक	सर्टिफाइड साइबर सिक्योरिटी मैनेजर (Certified Cyber Security Manager – CCSM)
पाठ्यक्रम कोड	
पात्रता	ग्रेजुएट
प्रमाणन	म.प्र. राज्य मुक्त विद्यालय शिक्षा बोर्ड द्वारा प्रदान
अध्ययन मोड	ई-लर्निंग (ऑनलाइन)
अवधि	06 माह
मॉड्यूल	06
शिक्षण समय/कक्षाएँ	प्रत्येक मॉड्यूल में 08 कक्षाएँ; कुल 06 मॉड्यूल मिलाकर कुल 48 कक्षाएँ शामिल हैं।

असाइनमेंट	1
मूल्यांकन/परीक्षा	परीक्षा का आयोजन म.प्र. राज्य मुक्त विद्यालय शिक्षा बोर्ड के निर्देशानुसार किया जाएगा।
	परीक्षा प्रारूप और विवरण मॉड्यूल संख्या :03 परीक्षा संख्या :01 मोड: ऑनलाइन प्रारूप: बहुविकल्पीय प्रश्न
संसाधन	अभ्यर्थी के पास सक्रिय इंटरनेट कनेक्टिविटी वाला स्मार्टफोन/कंप्यूटर होना चाहिए
अध्ययन सामग्री	ऑनलाइन अध्ययन सामग्री, व्यावहारिक वीडियो आदि उपलब्ध कराए जाएंगे
शुल्क	17110

4. पाठ्यक्रम एवं पाठ्यचर्या:

मॉड्यूल-1: साइबर सुरक्षा

- साइबरस्पेस को परिभाषित करना और साइबरस्पेस का विनियमन।
- कंप्यूटर और वेब-प्रौद्योगिकी का अवलोकन।
- भारतीय साइबरस्पेस की वास्तुकला, संचार और वेब प्रौद्योगिकी।
- इंटरनेट, वर्ल्ड वाइड वेब और इंटरनेट का आगमन।
- साइबर सुरक्षा की अवधारणा, सिद्धांत और आवश्यकता।
- साइबर सुरक्षा के मुद्दे और चुनौतियाँ।
- साइबर हमले: साइबर हमलों के विभिन्न रूप।

मॉड्यूल-2: साइबर कानून और साइबर स्पेस के लिए कानूनी ढांचा

- साइबर विधिशास्त्र और साइबर कानून का परिचय।
- साइबरस्पेस का परिचय, वास्तुकला और डिजिटल डिवाइड।
- भारत में ई-कॉमर्स और ई-गवर्नेंस का विनियमन।
- डेटा संरक्षण और ऑनलाइन गोपनीयता।
- गोपनीयता और डेटा संरक्षण के मुद्दे।
- इंटरनेट पर व्यक्तिगत पहचान के लिए खतरे।
- आईटी अधिनियम, 2000 के तहत गोपनीयता और डेटा संरक्षण के प्रावधान।

मॉड्यूल-3: कंप्यूटर नेटवर्क और संसाधन

- कंप्यूटर नेटवर्किंग।
- वास्तुकला और घटक।

- आईओटी (IOT) ।

मॉड्यूल-4: कंप्यूटर अपराध और साइबर अपराध

- साइबर अपराधों का वर्गीकरण ।
- सामान्य साइबर अपराध: कंप्यूटर और मोबाइल को लक्षित करने वाले अपराध, महिलाओं और बच्चों के खिलाफ अपराध, और वित्तीय धोखाधड़ी ।
- साइबर हमलों के विभिन्न रूप: सोशल इंजीनियरिंग, मैलवेयर और रैंसमवेयर हमले ।
- साइबर अपराधों की रिपोर्टिंग, उपचारात्मक उपाय और कानूनी परिप्रेक्ष्य ।
- आईटी अधिनियम 2000 और उसके संशोधन, साइबर अपराध और अपराध ।

मॉड्यूल-5: वेबसाइट और नेटवर्क सुरक्षा कार्यान्वयन और ऑडिट

- मौलिक सिद्धांत ।
- भेद्यता मूल्यांकन ।
- प्रवेश परीक्षण (Penetration testing) ।
- व्यावहारिक - सुरक्षा नियंत्रणों का कार्यान्वयन: वेबसाइट सुरक्षा, नेटवर्क सुरक्षा, सिस्टम सुरक्षा ।

मॉड्यूल-6: डिजिटल उपकरण सुरक्षा, उपकरण और साइबर सुरक्षा के लिए प्रौद्योगिकियाँ

- एंड पॉइंट डिवाइस और मोबाइल फोन सुरक्षा ।
- पासवर्ड नीति और सुरक्षा पैच प्रबंधन ।
- डेटा बैकअप और तृतीय-पक्ष सॉफ्टवेयर का प्रबंधन ।
- साइबर सुरक्षा की सर्वोत्तम प्रथाएँ ।
- होस्ट फ़ायरवॉल और एंटी-वायरस का महत्व और प्रबंधन ।
- वाई-फाई सुरक्षा और बुनियादी सुरक्षा नीतियों का विन्यास ।