संगणक शास्त्र प्रशाळा, कवयित्री बहिणाबाई चौधरी उत्तर महाराष्ट्र विद्यापीठातर्फे आयोजित प्रमाणपत्र अभ्यासक्रमात सहभागी होणेबाबत...

कवयित्री बहिणाबाई चौधरी उत्तर महाराष्ट्र विद्यापीठ परिक्षेत्रातील सर्व इच्छुक विद्यार्थी / व्यक्ती यांच्यासाठी फेब्रुवारी व मार्च या कालावधीत कवयित्री बहिणाबाई चौधरी उत्तर महाराष्ट्र विद्यापीठ, संगणक शास्त्र प्रशाळा येथे खालील प्रमाणपत्र अभ्यासक्रमांचे आयोजन करण्यात येणार आहे.

१) Cyber security certificate course: शनिवार, रविवार (चार आठवडे)
अभ्यासक्रमाचा एकूण कालावधी : आठ दिवस (४५ तास) शुल्क: रु. ५००० मात्र

२) Digital Ethical Hacking certificate course:शनिवार, रविवार(चार आठवडे)
अभ्यासक्रमाचा एकूण कालावधी : आठ दिवस (४५ तास) शुल्क: रु.७५०० मात्र

वरील अभ्यासक्रमांचा कालावधी खालीलप्रमाणे:

Sr. No.	Day	Date
1	Saturday	
2	Sunday	
3	Saturday	
4	Sunday	
5	Saturday	
6	Sunday	
7	Saturday	
8	Sunday	

संगणक जगतामध्ये अतिशय आवश्यक असे हे अभ्यासक्रम असून IT Industry साठी लागणारी कौशल्य वृद्धिंगत होण्यासाठी हे अभ्यासक्रम उपयुक्त आहे. या अभ्यासक्रमामुळे आपल्याला विविध क्षेत्रात करिअर संधी उपलब्ध होऊ शकतील.

सर्व अभ्यासक्रमाबद्दल सविस्तर माहिती खाली दिलेली आहे.

विशेष सूचना:

१) पूर्वी नोंदणी केलेल्यांनाही परत नोंदणी करणे आवश्यक आहे.

२) online नोंदणी झाल्यावर कोर्स फीच्या किमान ५०% रक्कम जोपर्यंत संगणक शास्त्र प्रशाळेत रोखीने प्रत्यक्ष जमा होत नाही तोवर नोंदणी नक्की झाली असे समजले जाणार नाही.

३) सर्व अभ्यासक्रमांना मर्यादित जागा असून शुल्कासहित प्रथम नोंदणी करणाऱ्यांना प्रथम

प्राधान्य असेल.

सर्व इच्छुक विद्यार्थी / व्यक्तींनी अधिक माहितीसाठी संपर्क करावा.

संगणक शास्त्र प्रशाळा,

क. ब. चौ. उत्तर महाराष्ट्र विद्यापीठ, जळगाव. (०२५७-२२५७४५३)

प्रा. कविता तु. पाटील (संपर्क क्र. ९९७०९१३७८९) इमेल: meetpatilkavita@gmail.com

सर्व इच्छुक व्यक्तींनी खाली दिलेल्या लिंक वर नाव नोंदणी करावी.

लिंक: : https://forms.gle/LJmhQi3v4XYP6CQ56

नोंदणीची अंतिम तारीख-20/11/2021 पर्यंत.

सूचना: कोर्स ऑनलाइन मोडमध्ये घेण्यात येईल

List of topics - Cyber security certificate course

1) Certificate in Cyber Security-

1. Introduction to Cyber Security, 2. Latest Technological Trends, 3. Basics of Networking, 4. Virtualization and installation of OS on virtual Box, 4. Passwords, 5. Web browser security, 6. Firewall And UTM, 7. Physical Security Closed circuit television cameras (CCTV), 8. Mobile Security, 9. Email Security, 10. Malware, 11. Cryptography, 12. Wireless Security,13. Ethical Hacking, 14. Google Hacking, 15. Virtualization and Cloud Computing, 16. Cloud Computing, 17. Cyber Crime and Cyber Laws, 18. Cyber laws (Information Technology Act 2000 & 2008), 19. ISO 27001, 20. IP based communication: (VOIP), 20. Protection of information Assets, Planning and implementation of BC/DR, 21. Make reports based on test results and make enhancements to existing security solutions, 22. Manage your work to meet requirements, 23. Work effectively with colleagues, 24. Maintain a healthy, safe and secure. 25.

SR NO	Modules
1	Introduction to Cyber Security
2	Latest Technological Trends
3	Basics of Networking
4	Virtualization and installation of OS on virtual Box.
5	Passwords
6	Web browser security
7	Firewall And UTM
8	Physical Security Closed circuit television cameras (CCTV)
9	Mobile Security
10	Email Security
11	Malware
12	Cryptography
13	Wireless Security
14	Ethical Hacking
15	Google Hacking
16	Virtualization and Cloud Computing
17	Cloud Computing
18	Cyber Crime and Cyber Laws
19	Cyber laws (Information Technology Act 2000 & 2008)
20	ISO 27001
21	IP based communication: (VOIP)
22	Protection of information Assets, Planning and implementation of BC/DR
23	Make reports based on test results and make enhancements to existing security solutions
24	Manage your work to meet requirements
25	Work effectively with colleagues
26	Maintain a healthy, safe and secure working environment

working environment.

List of topics -Digital Ethical Hacking certificate course

1) **Certificate in Digital Ethical Hacking-**

1. Introduction to Hacking, 2. Information Gathering / Vulnerability Scanning,3. Malwares (Virus, Worm, Trojan…), 4. System Hacking, 5. Sniffing, 6. Site and Web server Hacking, 7. SQL Injection and Cross Site Scripting, 8. Buffer Overflow, 9. Multi-Platform (cross-platform) System Hacking 10. Mobile Pentesting ,11. Network DOS and DDOS, 12. Cryptography, Penetration Testing IDS / IPS and Firewall

Sr No	Formal structure of the Course
1	Introduction to Hacking
2	Information Gathering / Vulnerability Scanning
3	Malwares (Virus, Worm, Trojan…)
4	System Hacking
5	Sniffing
6	Site and Web server Hacking
7	SQL Injection and Cross Site Scripting
8	Buffer Overflow
9	Multi-Platform (cross-platform) System Hacking and
10	Mobile Pen testing
11	Network DOS and DDOS
12	Cryptography
13	Penetration Testing IDS / IPS and Firewall
14	Make reports based on test results and make enhancements to existing security solutions
15	Manage your work to meet requirements
16	Work effectively with colleagues
17	Maintain a healthy, safe and secure working environment