جمهوری اسلامی ایران

وزارت کار و امور اجتماعی

سازمان آموزش فنی و حرفه ای کشور

استاندارد مهارت و آموزشی

مهندس کامپیوتردر امنیت کسب و کار الکترونیکی

گروه برنامه ریزی درسی فناوری اطلاعات

تاریخ شروع اعتبار: ۱۳۸۴/۶/۱

کد استاندارد: ۰-۲۳/۹۷/۱/۲

دفتر طرح و برنامه های درسی: تهران- خیابان آزادی- خ خوش شمالی- تقاطع خوش و نصرت - ساختمان فناوری اطلاعات و ارتباطات- طبقه چهارم
تلفن: ۶۶۹۴۴۱۱۹ و۶۶۹۴۴۱۲۰ دورنگار: ۶۶۹۴۴۱۱۷
کدپستی: ۱۴۵۷۷۷۷۳۶۳
EMAIL:DEVELOP@IRANTVTO.IR

از کلیه صاحب نظران تقاضا دارد پیشنهادات و نظرات خود را درباره این سند آموزشی به نشانی‌های مذکور اعلام نمایند.

معاونت پژوهش و برنامه ریزی : تهران-خیابان آزادی- نبش چهارراه خوش- سازمان آموزش فنی و حرفه‌ای کشور- طبقه پنجم
تلفن:۶۶۹۴۱۵۱۶ دورنگار: ۶۶۹۴۱۲۷۲
کدپستی: ۱۳۴۵۶۵۳۸۶۸
EMAIL: INFO@IRANTVTO.IR

سازمان آموزش فنی و حرفه ای کشور

نام شغل : مهندس کامپیوتردر امنیت کسب و کار الکترونیکی

خلاصه استاندارد

تعریف مفاهیم سطوح یادگیری

آشنایی: به مفهوم داشتن اطلاعات مقدماتی/**شناسایی:** به مفهوم داشتن اطلاعات کامل/ **اصول :** به مفهوم مبانی مطالب نظری/ **توانایی:** به مفهوم قدرت انجام کار

مشخصات عمومی شغل:

مهندس کامپیوتردر امنیت کسب و کار الکترونیکی کسی است که روشهای بنیادین مورد استفاده در کاهش مخاطرات امنیتی E-Business را بوجود آورد و ایمن سازی کاربران تحت وب ، سرویس دهنده ها و ارتباطات و کنترل استفاده از فایروالها و تاییدیه های دیجیتال را انجام می دهد. همچنین از عهده بررسی و شناخت Information Security درمهندسی نرم افزار ، کار با نیازمندی های Security ، کار با Legal و Ethical و Professional Issues در Information Security ، کار با Risk Management ، کار با Assessing وControlling Risk در Risk Management ، کار با Blueprint برای Security ، Planning برای Continuity ، کار با تکنولوژی های Security ، کار با Physical Security ، پیاده سازی Security ، انجام Information Security Maintenance ، کار با Security و Personnel بر خواهد آمد. مهندس کامپیوتر E-Security مراکز کامپیوتر و IT در تیم های مهندسی نرم افزار برای طراحی و پیاده سازی سیستم های مهندسی نرم افزار برای امنیت M-Commerce و E-Commerce و E-Business و E-Government و E-Learning و موارد دیگر در مراکز میتواند انجام وظیفه کند.

ویژگی های کارآموزورودی:

حداقل میزان تحصیلات : مهندس کامپیوتر

حداقل توانایی جسمی: متناسب با نوع شغل

مهارت های پیش نیاز این استاندارد: –

طول دوره آموزشی :

طول دوره آموزش	**:**	**۲٦٤**	**ساعت**
ـ زمان آموزش نظری	**:**	**۲۳**	**ساعت**
ـ زمان آموزش عملی	**:**	**۸۱**	**ساعت**
ـ زمان کارآموزی در محیط کار	**:**	**۸۰**	**ساعت**
ـ زمان اجرای پروژه	**:**	**۸۰**	**ساعت**
ـ زمان سنجش مهارت	**:**	–	**ساعت**

روش ارزیابی مهارت کارآموز:

۱- امتیاز سنجش نظری(دانش فنی): ۲۵٪

۲-امتیاز سنجش عملی : ۷۵٪

۱-۲- امتیاز سنجش مشاهده ای: ۱۰٪

۲-۲- امتیاز سنجش نتایج کار عملی: ۶۵٪

ویژگیهای نیروی آموزشی:

حداقل سطح تحصیلات : لیسانس مرتبط

سازمان آموزش فنی و حرفه ای کشور

نام شغل: مهندس کامپیوتر در امنیت کسب و کار الکترونیکی

فهرست توانایی های شغل

ردیف	عنوان توانایی
۱	توانایی بررسی و شناخت Information Security درمهندسی نرم افزار
۲	توانایی کار با نیازمندی های Security
۳	توانایی کار با Legal و Ethical و Professional Issues در Information Security
۴	توانایی مدیریت مخاطرات
۵	توانایی کار با Assessing وControlling Risk در Risk Management
۶	توانایی کار با Blueprint برای Security
۷	توانایی Planning برای Continuity
۸	توانایی کار با تکنولوژی های Security
۹	توانایی کار با Physical Security
۱۰	توانایی پیاده سازی Security
۱۱	توانایی انجام Information Security Maintenance
۱۲	توانایی کار با Security و Personnel

سازمان آموزش فنی و حرفه ای کشور

نام شغل: مهندس کامپیوتر در امنیت کسب و کار الکترونیکی

اهداف و ریزبرنامه درسی

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱	**توانـــایی بررســـی و شـــناخت Information Security درمهندسی نرم افزار**	۱/۵	۳	٤/۵
۱-۱	آشنایی با مفاهیم اولیه و اساسی information security			
۱-۲	آشـــنایی بـــا بررســـی computer security وزیـــر سیـــستم آن information security			
۱-۳	آشنایی با موارد کلیدی و مشکلات information security			
۱-۴	شناســـایی اصـــول بررســـی security systems و نقـــش آن در development life cycle در مهندسی نرم افزار			
۱-۵	شناسایی اصول بررسـی مـوارد پیـشرفته و حرفـه ای information security درساختار سازمان			
۲	**توانایی کار با نیازمندی های Security**	۱/۵	۳	٤/۵
۲-۱	شناسایی اصول تنظیم نیازمندیهای business برای information security			
۲-۲	شناسایی اصول برنامه ریزی و طرح موفق information security برای پاسخ به مدیر عمومی و مدیر کامپیوتر و IT			
۲-۳	شناسـایی اصـول بررسـی threats posed بـرای information security			
۲-۴	شناسایی اصول بررسی تفاوت بین تهدیـد information systems و حمله به information systems			
۳	**توانایی کار با Legal و Ethical و Professional Issues در Information Security**	٤	۵	۹
۳-۱	شناسایی اصول بررسی تفاوت بین laws و ethics			
۳-۲	شناسـایی اصـول بررسـی و کـار بـا national laws کـه بـرای information security			
۳-۳	شناسایی اصول کار با role های یک فرهنگ بـرای information security			
٤	**توانایی مدیریت مخاطرات**	۱/۵	٦/۵	۸
۴-۱	شناســایی اصــول کــار بــا risk management و role هــا در SecSDLC			
۴-۲	شناسایی اصول کاربا risk و شناسایی آن			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۳-۴	شناسایی اصول ارزیابی risk در احتمال رویداد و گیر انداختن در یک سازمان			
۴-۴	شناسایی اصول اعمال دیدگاه سخت در شناسایی documenting risk و assessment			
۵	**توانایی کار با Assessing وControlling Risk در Risk Management**	۱/۵	۳	٤/٥
۵-۱	شناسایی اصول تشخیص چگونگی risk control برای نیاز سازمان			
۵-۲	شناسایی اصول کار با گزینه های استراتژی risk mitigation برای controlling risks			
۵-۳	شناسایی اصول کارشناخت جزئیاتی که برای classify Controls بکار میروند			
۵-۴	شناسایی اصول کاربا آگاهی برای conceptual frameworks که موجود است و توانا هستند برای فرمول risk controlsبرای ارزیابی کردن قیمت آنالیز سودمند			
۵-۵	شناسایی اصول انجام maintain و perpetuate برای risk controls			
٦	**توانایی کار با Blueprint برای Security**	۱/۵	٦/٥	۸
۶-۱	شناسایی اصول کاربا management's responsibilities و role در development و maintenance و enforcement در خصوص سیاست information security و standards وguidelines			
۶-۲	شناسایی اصول کاربا سیاستهای کلی سازمان بین information security و requirements و اهداف و سیاست های ویژه سازمان			
۶-۳	شناسایی اصول کار با blueprint یک information security در خصوص major components			
۶-۴	شناسایی اصول کاربا policies و standards و عادات استفاده ازآموزش و کاآموزی وبرنامه های آگاهی			
۶-۵	شناسایی اصول کار با information security architecture مناسب			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۷	**توانایی Planning برای Continuity**	۱/۵	٦/۵	۸
۷-۱	شناسایی اصول کار با contingency planning و incident response planning و disaster recovery planning و business continuity plans			
۷-۲	شناسایی اصول کار با المنت های business impact analysis و information که برای attack profile گردآوری میشوند			
۷-۳	شناسایی اصول کار با اجزاء incident response plan			
۸	**توانایی کار با تکنولوژی های Security**	۱/۵	۳	٤/۵
۸-۱	شناسایی اصول کار با انواع firewalls			
۸-۲	شناسایی اصول دستیابی به firewall implementation			
۸-۳	شناسایی اصول دستیابی به dial-up access وprotection			
۸-۴	شناسایی اصول کار با دو عامل intrusion detection systems یعنی Identify و describe			
۸-۵	شناسایی اصول کار با دو استراتژی behind intrusion detection systems			
۹	**توانایی کار با Physical Security**	۱/۵	۳	٤/۵
۹-۱	شناسایی اصول کار با نیازمندی های physical security			
۹-۲	شناسایی اصول شناسایی تهدید برای information security و unique کردن physical security			
۹-۳	شناسایی اصول کار با موارد کلیدی physical security برای انتخاب یک facility site			
۹-۴	شناسایی اصول کار با اجزای physical security monitoring			
۹-۵	شناسایی اصول کار با المنت های لازم access control در داخل حوزه facilities management			
۹-۶	شناسایی اصول کار با criticality در خصوص برنامه های fire safetyبرای همه برنامه های physical security			

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۰	**توانایی پیاده سازی Security**	٤	۲۰	۲٤
۱۰-۱	شناسایی اصول برنامه ریزی و طرح security سازمان با یک project plan			
۱۰-۲	شناسایی اصول بررسی سازمان از نظر security با استفاده از آدرس دهی project plan			
۱۰-۳	شناسایی اصول تهیه significant role و اهمیت project manager در موفقیت information security project			
۱۰-۴	شناسایی اصول گردآوری نیازمندی های professional project management برای complex projects			
۱۰-۵	شناسایی اصول گردآوری استراتژی های تکنیکی و مدلها برای پیاده سازی project plan			
۱۰-۶	شناسایی اصول گردآوری مسائل غیر تکنیکی که چهره سازمان را در هر زمان تغییر میدهند			
۱۱	**توانایی انجام Information Security Maintenance**	۱/۵	۱۵	۱٦/۵
۱۱-۱	شناسایی اصول شناخت نیازمندی ها برای ادامه حفظ maintenance برای برنامه information security			
۱۱-۲	شناسایی اصول کار با مدلهای security management توصیه شده			
۱۱-۳	شناسایی اصول کار با مدلهای گوناگون برای برنامه کامل maintenance			
۱۱-۴	شناسایی اصول کار با فاکتورهای کلیدی برای monitoring برای محیط های external و internal			
۱۱-۵	شناسایی اصول انجام planning وrisk assessment در یک information security maintenance			
۱۱-۶	شناسایی اصول کار vulnerability assessment و آموزش information security maintenance			
۱۱-۷	شناسایی اصول کار آموزش build readiness و and review procedures در داخل information security maintenance			

نام شغل: مهندس کامپیوتر در امنیت کسب و کار الکترونیکی

اهداف و ریزبرنامه درسی

شماره	شرح	زمان آموزش		
		نظری	عملی	جمع
۱۲	**توانایی کار با Security و Personnel**	**۱/۵**	**٦/۵**	**۸**
۱۲-۱	شناسایی اصول بررسی مکان و زمان اجرای عملیات information security در یک سازمان			
۱۲-۲	شناسایی اصول یافتن کارمندانی که وابستگی و ملاک عملیاتی information security هستند			
۱۲-۳	شناسایی اصول کار برروی استوار نامه حرفه ای که در information security field میتواند برقرار گردد			
۱۲-۴	شناسایی اصول کار با مواردی که میتواند سیاست گذاری برای کارمندان را قانونی کند و تمرین برای پشتیبانی information security			
۱۲-۵	شناسایی اصول کار اقدامات حیاطی لازم برای افراد غیر کارمند			
۱۲-۶	شناسایی اصول تنظیم مستندات قانونمند کردن نیازها برای دسته بندی وظایف			
۱۲-۷	شناسایی اصول تنظیم مستندات نیازمندی های ویژه برای personnel data بسیاتر محرمانه			

سازمان آموزش فنی و حرفه ای کشور

نام شغل : مهندس کامپیوتر در امنیت کسب و کار الکترونیکی

فهرست استاندارد تجهیزات، ابزار ، مواد و وسایل رسانه ای

ردیف	مشخصات فنی	تعداد	شماره
۱	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Windows Xp	۸	
۲	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Windows 2003 server	۸	
۳	کامپیوتر پنتیوم IV کامل یا مشابه یا بالاتر برای Linux	۸	
۴	CD های MS Office Xp	۸	
۵	Cisco PIX FireWall	۸	
۶	چاپگر	۸	
۷	CDهای آموزشی	۸	
۸	پوستر		

فهرست منابع و نرم افزارهای آموزشی

ردیف	شرح
۱	کلیه سایتهای اینترنتی بهترین مرجع و منبع برای امنیت کسب و کار الکترونیک میباشند.
۲	http://www.cisco.com
۳	http://www.symantec.com
۴	http://www.mcafee.com
۵	http://www.redhat.com
۶	http://www.microsoft.com
۷	http://www.astalavista.com
۸	http://www.antivirus.com
۹	http://www.oracle.com
۱۰	انواع کتابها و نرم افزارهای آموزشی مربوط به Hack وCrackو Security و Virus وFirewall و مدیریت نیروها و امکانات در وضعیتهای بحرانی
۱۱	بانکها و موسسات مالی
۱۲	شرکتهای کارگذاری الکترونیکی
۱۳	فروشگاههای الکترونیکی
۱۴	حراجیهای الکترونیکی
۱۵	بورس نفت
۱۶	بورس ارز
۱۷	بورس کالاهای صنعتی
۱۸	بورس کالاهای کشاورزی
۱۹	بورس اوراق بهادار
۲۰	شرکتهای سرمایه گزاری
۲۱	شرکتهای سرویس دهنده اینترنت (ISP)و(ICP)