جمهوری اسلامی ایران
وزارت تعاون، کار و رفاه اجتماعی

سازمان آموزش فنی و حرفه‌ای کشور

معاونت پژوهش، برنامه‌ریزی و سنجش مهارت

دفتر پژوهش، طرح و برنامه‌ریزی درسی

استاندارد آموزش شایستگی

کارآگاهی امنیت شبکه

گروه شغلی

فناوری اطلاعات

کد ملی آموزش شایستگی

۱	۷	۱	۰	۹	۵	۰	۳	۵	۴	۳	۲	۵	۲
نسخه	شناسه شایستگی			شناسه شغل			شناسه گروه		سطح مهارت		Isco-۰۸		

۲۵۲۳-۵۳-۰۱۹-۱

تاریخ تدوین استاندارد : ۹۳/۴/۱

تدوین محتوا و تصویب :

کد استاندارد شایستگی: ۱-۰۱۹-۵۳-۲۵۲۳

اعضاء کمیسیون تخصصی:

مهندس داریوش اسماعیلی کارشناس ارشد مدیریت استراتژیک در فناوری اطلاعات- مدرس دانشگاه جامع علمی کاربردی – مشاور فنی گروه صنعتی صاب- مدیر گروه فناوری اطلاعات دانشگاه WWS (World Wide Since) مالزی– عضو کلوپ مدیران مشاور در خاور میانه

مهندس سارنگ قربانیان کارشناس ارشد فناوری اطلاعات – مدیر گروه IT و مدرس دانشگاه جامع علمی کاربردی–

مهندس علی ثاقب کارشناس ارشد فناوری اطلاعات –مدرس دانشگاه جامع علمی کاربردی –معاون اداره کل طرح و مهندسی سوئیچ زیرساخت (وزارت ارتباطات)

مهندس رضا حاتمیان کارشناس ارشد فناوری اطلاعات –مدیر گروه IT و مدرس دانشگاه جامع علمی کاربردی –مشاور فناوری اطلاعات سازمان انتقال خون ایران

مهندس رامین مولاناپور کارشناس ارشد فناوری اطلاعات- مدرس دانشگاه جامع علمی کاربردی – عضو گروه دفتر برنامه ریزی و تالیف آموزش های فنی و حرفه ای و کاردانش-

مهندس حسن سلیمانی کارشناس فناوری اطلاعات –مدرس دانشگاه جامع علمی کاربردی– مدیر ارشد سایت شرکت رجاء

مهندس امیرعباس ممتاز کارشناس ارشد فناوری اطلاعات (امنیت شبکه)–مدرس دانشگاه جامع علمی کاربردی

مهندس شهرام شکوفیان کارشناس ارشد فناوری اطلاعات- رئیس کمیته برنامه ریزی درسی فناوری اطلاعات سازمان آموزش فنی وحرفه ای کشور

حوزه های حرفه ای و تخصصی همکار برای تدوین برنامه آموزش :

دفتر طرح و برنامه درسی سازمان آموزش فنی و حرفه ای کشور

فرآیند اصلاح و بازنگری :

-محتوای علمی

-تجهیزات

- تغییرات تکنولوژی

-نیاز بازار کار

- تقاضای متولیان اجرا و سیاستگذار

آدرس دفتر طرح و برنامه های درسی

تهران – خیابان آزادی ، خیابان خوش شمالی ، نبش خیابان نصرت ، ساختمان شماره ۲ ، سازمان آموزش فنی و حرفه‌ای کشور ، پلاک ۹۷

دورنگار ٦٦٩٤٤١١٧ تلفن ۹ – ٦٦٥٦٩٩٠٠

مشخصات استاندارد شایستگی

عنوان استاندارد شایستگی:
کار1گاهی امنیت شبکه
شرح استاندارد شایستگی :
این استاندارد دربر گیرنده و پوشش دهنده شیوه استانداردی مناسب به منظور عملیات کار1گاهی امنیت شبکه است. عناصر شایستگی بررسی و تشخیص مقدماتی و تکمیلی با امنیت شبکه، بررسی و تشخیص قوانین و مقررات حوزه سایبر ، بررسی و تشخیص جرائم رایانه ایی و سایبری وآشنایی با نهاد های رسیدگی کننده ، بررسی و تشخیص روش های غیر مجاز بهره برداری از اطلاعات در سطح شبکه های رایانه ایی ، بررسی و تشخیص انواع روش های تهاجم در شبکه های ارتباطی و انتقال دیتا ، بررسی و تشخیص آلودگی های الکترونیکی و نحوه مقابله و رصد آنها در سطح شبکه های ارتباطی در آن تشریح شده است. همچنین معیار عملکرد هر عنصر شایستگی نیز بر اساس استاندارد ملی حرفه ای احصا، گردیده است.
ویژگی های کارآموز ورودی :
حداقل میزان تحصیلات : دارا بودن دیپلم متوسط کامپیوتر کار و دانش – دیپلم متوسط کامپیوتر هنرستان های فنی و حرفه ای- برای سایر دیپلم ها با گذراندن دوره های مهارت های هفت گانه ICDL یا گذراندن دوره های آموزشی ICDL(درجه ۲و۱) یا کاربر رایانه یا رایانه کار درجه ۲ **حداقل توانایی جسمی و ذهنی : سلامت کامل جسمانی و روانی** **شایستگی پیش نیاز : گذراندن بسته نصب و نگهداری شبکه**
طول دوره آموزش :
-طول دوره آموزش : ٦٤ ساعت **ـ زمان آموزش نظری : ١٦ ساعت** **ـ زمان آموزش عملی : ٤٨ ساعت**
بودجه بندی ارزشیابی (به درصد)
- کتبی : ۲۵٪ **- عملی :٦٥٪** **- اخلاق حرفه ای :۱۰٪**
صلاحیت های حرفه ای مربیان :
لیسانس مهندسی کامپیوتر یا فناوری اطلاعات با حداقل سه سال سابقه کار مرتبط

استاندارد آموزش

- برگه‌ی عناصر شایستگی و معیارهای عملکرد

عنصر شایستگی	معیار عملکرد
۱- بررسی و تشخیص مقدماتی و تکمیلی با امنیت شبکه	۱ ـ ۱ - بررسی و شناسایی امینت اطلاعات ۱ ـ ۲ - بررسی امنیت اطلاعات از دید محرمانگی – جامعیت و صحت ۱ ـ ۳ - بررسی وشناسایی مدل های امنیت اطلاعات در سطح شبکه های کامپیوتری ۱ ـ ۴ - بررسی وشناسایی معماری های امنیتی با توجه به استاندارد های مورد نظر ۱ ـ ۵ - پیاده سازی معماری امنیتی در سطح شبکه ها از دیدگاه استاندارد
۲- بررسی و تشخیص قوانین و مقررات حوزه سایبر	۲-۱- بررسی قوانین عمومی و خصوصی ۲-۲- بررسی و شناسایی قوانین مجازاتی ۲-۳- بررسی و شناسایی قوانین مرتبط با جرائم سایبری ۲-۴- بررسی و شناسایی قوانین مرتبط با جرائم سایبری در سایر کشور ها
۳- بررسی و تشخیص جرائم رایانه ایی و سایبری وآشنایی با نهاد های رسیدگی کننده	۳-۱- بررسی جرم ۳-۲- طبقه بندی جرم از دیدگاه سازمان یافته ۳-۳- بررسی و شناسایی جرائم سایبری ۳-۴- بررسی مصادیق محتوای مجرمانه در فضای سایبر ۳-۵- بررسی و شناسایی نظام رسیدگی به جرائم سایبری ۳-۶- بررسی و شناسایی حیطه وظایف و عملکرد پلیس فضای تولید و تبادل اطلاعات (فتا) ۳-۷- نحوه تعامل با این دستگاه در موارد خاص
۴- بررسی و تشخیص روش های غیر مجاز بهره برداری از اطلاعات در سطح شبکه های رایانه ایی	۴-۱- بررسی امنیت اطلاعات از دید محرمانگی ۴-۲- آشنایی با نقض محرمانگی در انتقال اطلاعات ۴-۳- بررسی روش های ورود مجاز ۴-۴- بررسی و شناسایی روش های ورود غیر مجاز در سطح شبکه ها ۴-۵- بررسی و شناسایی نقل و انتقال داده های غیر مجاز در سطح شبکه ها ۴-۶- بررسی و شناسایی بهره برداری غیر مجاز از امکانات و تجهیزات شبکه ۴-۷- بررسی تردد غیر مجاز در سطح شبکه های ارتباطی و انتقال داده

عنصر شایستگی	معیار عملکرد
۵- بررسی و تشخیص انواع روش های تهاجم در شبکه های ارتباطی و انتقال دیتا	۵-۱- بررسی و تشخیص حملات انکار سرویس ۵-۲- بررسی و تشخیص حملات جلوگیری از انتقال دیتا در سطح شبکه های ارتباطی و رایانه ایی ۵-۳- بررسی و تشخیص حملات تغییر در متن پیام دیتا در سطح شبکه های ارتباطی و رایانه ایی ۵-۴- بررسی و تشخیص حملات تغییر در آدرس مقصد یا ایستگاه های میانی در سطح شبکه های ارتباطی و رایانه ایی ۵-۵- بررسی و تشخیص حملات جعل آدرس فیزیکی در سطح شبکه های ارتباطی و رایانه ایی ۵-۶- بررسی و تشخیص حملات جعل اینترنتی در سطح شبکه های ارتباطی و رایانه ایی
۶- بررسی و تشخیص آلودگی های الکترونیکی و نحوه مقابله و رصد آنها در سطح شبکه های ارتباطی	۶-۱- بررسی و تشخیص انواع آلودگی های الکترونیکی ۶-۲- بررسی و تشخیص ویروس ها ۶-۳- بررسی و تشخیص تروجان ها ۶-۴- بررسی و تشخیص کرم ها ۶-۵- بررسی و تشخیص جاسوس افزار ها (اسپای ویر) ۶-۶- بررسی و تشخیص روت کیت ها ۶-۷ – بررسی و تشخیص ویروس های هوشمند ۶-۸ – بررسی و تشخیص ابزارهای نفوذ و حمله در سطح سایبر ۶-۹- بررسی سیستم های تشخیص آلودگی و مقابله با آنها

استاندارد آموزش

برگه تحلیل آموزش

دانش :	**زمان اسمی آموزش:۱۶ ساعت**

محرمانگی – جامعیت و صحت

معماری های امنیتی با توجه به استاندارد های مورد نظر

معماری امنیتی در سطح شبکه ها از دیدگاه استاندارد

قوانین عمومی و خصوصی

قوانین مجازاتی

قوانین مرتبط با جرائم سایبری در جمهوری اسلامی ایران

قوانین مرتبط با جرائم سایبری در سایر کشور ها

جرم

جرائم سایبری

نظام رسیدگی به جرائم سایبری در قوه قضاییه در جمهوری اسلامی ایران

انواع آلودگی های الکترونیکی

چگونگی بررسی و شناسایی امینت اطلاعات

چگونگی بررسی امنیت اطلاعات از دید محرمانگی – جامعیت و صحت

چگونگی بررسی وشناسایی مدل های امنیت اطلاعات در سطح شبکه های کامپیوتری

چگونگی بررسی وشناسایی معماری های امنیتی با توجه به استاندارد های مورد نظر

چگونگی پیاده سازی معماری امنیتی در سطح شبکه ها از دیدگاه استاندارد

نحوه بررسی قوانین عمومی و خصوصی

نحوه بررسی و شناسایی قوانین مجازاتی

نحوه بررسی و شناسایی قوانین مرتبط با جرائم سایبری در جمهوری اسلامی ایران

نحوه بررسی و شناسایی قوانین مرتبط با جرائم سایبری در سایر کشور ها

بررسی جرم

نحوه طبقه بندی جرم از دیدگاه سازمان یافته

نحوه بررسی و شناسایی جرائم سایبری

نحوه بررسی مصادیق محتوای مجرمانه در فضای سایبر

نحوه بررسی و شناسایی نظام رسیدگی به جرائم سایبری

نحوه بررسی و شناسایی حیطه وظایف و عملکرد پلیس فضای تولید و تبادل اطلاعات (فتا)

نحوه تعامل با این دستگاه در موارد خاص

بررسی امنیت اطلاعات از دید محرمانگی

نحوه آشنایی با نقض محرمانگی در انتقال اطلاعات

نحوه بررسی روش های ورود مجاز

نحوه بررسی و شناسایی روش های ورود غیر مجاز در سطح شبکه ها

نحوه بررسی و شناسایی نقل و انتقال داده های غیر مجاز در سطح شبکه ها

نحوه بررسی و شناسایی بهره برداری غیر مجاز از امکانات و تجهیزات شبکه

نحوه بررسی تردد غیر مجاز در سطح شبکه های ارتباطی و انتقال داده

نحوه بررسی و تشخیص حملات انکار سرویس

نحوه بررسی و تشخیص حملات جلوگیری از انتقال دیتا در سطح شبکه های ارتباطی و رایانه ایی

نحوه بررسی و تشخیص حملات تغییر در متن پیام دیتا در سطح شبکه های ارتباطی و رایانه ایی

نحوه بررسی و تشخیص حملات تغییر در آدرس مقصد یا ایستگاه های میانی در سطح شبکه های ارتباطی و رایانه ایی

نحوه بررسی و تشخیص حملات جعل آدرس فیزیکی در سطح شبکه های ارتباطی و رایانه ایی

نحوه بررسی و تشخیص حملات جعل اینترنتی در سطح شبکه های ارتباطی و رایانه ایی

نحوه بررسی و تشخیص انواع آلودگی های الکترونیکی

نحوه بررسی و تشخیص ویروس ها

نحوه بررسی و تشخیص تروجان ها

نحوه بررسی و تشخیص کرم ها

نحوه بررسی و تشخیص جاسوس افزار ها (اسپای ویر)

نحوه بررسی و تشخیص روت کیت ها

نحوه بررسی و تشخیص ویروس های هوشمند

نحوه بررسی و تشخیص ابزارهای نفوذ و حمله در سطح سایبر

نحوه بررسی سیستم های تشخیص آلودگی و مقابله با آنها

مهارت :	**زمان اسمی آموزش: ٤٨ ساعت**

تعین جرم با توجه به مستندات تصویب شده

تنظیم اطلاعات از دید محرمانگی

بهره برداری غیر مجاز از امکانات و تجهیزات شبکه

تردد غیر مجاز در سطح شبکه های ارتباطی و انتقال داده

تعامل با این دستگاه در موارد خاص

پیاده سازی معماری امنیتی در سطح شبکه ها از دیدگاه استاندارد

انجام بررسی و شناسایی امینت اطلاعات

انجام بررسی امنیت اطلاعات از دید محرمانگی – جامعیت و صحت

انجام بررسی وشناسایی مدل های امنیت اطلاعات در سطح شبکه های کامپیوتری

انجام بررسی وشناسایی معماری های امنیتی با توجه به استاندارد های مورد نظر

انجام پیاده سازی معماری امنیتی در سطح شبکه ها از دیدگاه استاندارد

انجام بررسی قوانین عمومی و خصوصی

انجام بررسی و شناسایی قوانین مجازاتی

انجام بررسی و شناسایی قوانین مرتبط با جرائم سایبری

انجام بررسی و شناسایی قوانین مرتبط با جرائم سایبری در سایر کشور ها

انجام بررسی جرم
بررسی طبقه بندی جرم از دیدگاه سازمان یافته
بررسی و شناسایی جرائم سایبری
بررسی مصادیق محتوای مجرمانه در فضای سایبر
بررسی و شناسایی نظام رسیدگی به جرائم سایبری
بررسی و شناسایی حیطه وظایف و عملکرد پلیس فضای تولید و تبادل اطلاعات (فتا)
انجام تعامل با این دستگاه در موارد خاص
انجام بررسی امنیت اطلاعات از دید محرمانگی
انجام بررسی نقض محرمانگی در انتقال اطلاعات
بررسی روش های ورود مجاز
بررسی و شناسایی روش های ورود غیر مجاز در سطح شبکه ها
بررسی و شناسایی نقل و انتقال داده های غیر مجاز در سطح شبکه ها
بررسی و شناسایی بهره برداری غیر مجاز از امکانات و تجهیزات شبکه
بررسی تردد غیر مجاز در سطح شبکه های ارتباطی و انتقال داده
بررسی و تشخیص حملات انکار سرویس
بررسی و تشخیص حملات جلوگیری از انتقال دیتا در سطح شبکه های ارتباطی و رایانه ایی
بررسی و تشخیص حملات تغییر در متن پیام دیتا در سطح شبکه های ارتباطی و رایانه ایی
بررسی و تشخیص حملات تغییر در آدرس مقصد یا ایستگاه های میانی در سطح شبکه های ارتباطی و رایانه ایی
بررسی و تشخیص حملات جعل آدرس فیزیکی در سطح شبکه های ارتباطی و رایانه ایی
بررسی و تشخیص حملات جعل اینترنتی در سطح شبکه های ارتباطی و رایانه ایی
بررسی و تشخیص انواع آلودگی های الکترونیکی
بررسی و تشخیص ویروس ها
بررسی و تشخیص تروجان ها
بررسی و تشخیص کرم ها
بررسی و تشخیص جاسوس افزار ها (اسپای ویر)
بررسی و تشخیص روت کیت ها
بررسی و تشخیص ویروس های هوشمند
بررسی و تشخیص ابزارهای نفوذ و حمله در سطح سایبر
بررسی سیستم های تشخیص آلودگی و مقابله با آنها

نگرش:

- دقت در انتخاب ابزار و تجهیزات و قطعات
- دقت در کار با ابزار و تجهیزات و قطعات
- رعایت اخلاق حرفه ای

- برگه استاندارد تجهیزات

ردیف	نام	مشخصات فنی و دقیق	تعداد	توضیحات
۱	رایانه مخصوص کلاینت	پنتیوم Core i۵ با Ram ٤G یا	۱	برای دو نفر
۲	رایانه مخصوص سرور	سوپر میکرو یا HP چند هسته ای با Ram ۸G یا بالاتر	٤	برای هر ٤ نفر
۳	دیتا پروژکتور و پرده دیتا	ویژه کارگاه	۱	برای کارگاه
٤	میز رایانه کلاینت	مجهز و جدید	۱	برای دو نفر
٥	میز سرور جهت اسمبل	مجهز و جدید	٤	هر سرور یک عدد
٦	صندلی گردان	آموزشی	۱	برای هر نفر
۷	چاپگر لیزری	سیاه و سفید یا رنگی	۱	برای کارگاه
۸	اسکنر	رنگی USB	۱	برای کارگاه
۹	تجهیزات مخابراتی اتصال	خطوط مناسب اتصال و تجهیزات	۱	برای کارگاه
۱۰	وایت برد	حداقل ۲ در ۲.٥ متر	۱	برای کارگاه
۱۱	رک ایستاده	حداقل ۱۸ یونیت	٤	هر سرور یک عدد
۱۲	رک دیواری برای تجهیزات	حداقل ٤ یونیت	٤	هر سرور یک عدد
۱۳	هاب باسیم	حداقل ۱٦ پورت جدید و	٤	هر سرور یک عدد
۱٤	سوییچ باسیم	حداقل ۱٦ پورت جدید و	٤	هر سرور یک عدد
۱٥	روتر باسیم	حداقل ۱٦ پورت جدید و	٤	هر سرور یک عدد
۱٦	بریج با سیم	جدید و استاندارد	٤	هر سرور یک عدد
۱۷	Access Point با سیم	جدید و استاندارد	٤	هر سرور یک عدد
۱۸	فایروال با سیم	سخت افزار جدید و استاندارد	٤	هر سرور یک عدد
۱۹	هاب بی سیم	جدید و استاندارد	٤	هر سرور یک عدد
۲۰	سوییچ بی سیم	جدید و استاندارد	٤	هر سرور یک عدد
۲۱	روتر بی سیم	جدید و استاندارد	٤	هر سرور یک عدد
۲۲	بریج بی سیم	جدید و استاندارد	٤	هر سرور یک عدد
۲۳	تکرار کننده	جدید و استاندارد	٤	هر سرور یک عدد
۲٤	فایروال بی سیم	سخت افزار جدید و استاندارد	٤	هر سرور یک عدد
۲٥	Access Point بی سیم	جدید و استاندارد	٤	هر سرور یک عدد
۲٦	Transceiver - infrared	انعکاسی جدید و استاندارد	٤	هر سرور یک عدد
۲۷	Transceiver - infrared	انعکاسی جدید و استاندارد	۸	هر کلاینت یک

۲۸	Transceiver - Bluetooth	جدید و استاندارد	٤	هر سرور یک عدد
۲۹	Transceiver - Bluetooth	جدید و استاندارد	۸	هر کلاینت یک عدد
۳۰	Transceiver - infrared	پخشی جدید و استاندارد	٤	هر سرور یک عدد
۳۱	Transceiver - infrared	پخشی جدید و استاندارد	۸	هر کلاینت یک
۳۲	Transceiver - infrared	P۲P جدید و استاندارد	٤	هر سرور یک عدد
۳۳	Transceiver - infrared	P۲P جدید و استاندارد	۸	هر کلاینت یک
۳٤	UPS + Stabilizer	خشک ، جدید و استاندارد	٤	هر سرور یک عدد
۳٥	UPS + Stabilizer	خشک ، جدید و استاندارد	۸	هر کلاینت یک
۳٦	دستگاه جوش فیوژن و اتصال دهنده کابلهای	جدید و استاندارد	۱	برای کارگاه
۳۷	کارت شبکه بی سیم	جدید و استاندارد	۱۲	هر سیستم یک عدد
۳۸	کارت شبکه باسیم	جدید و استاندارد	۱۲	هر سیستم یک عدد
۳۹	کارت شبکه نوری	جدید و استاندارد	۱۲	هر سیستم یک عدد
٤۰	آنتن Wi-Fi	جدید و استاندارد	٤	هر سرور یک عدد
٤۱	آنتن Wi-Max	جدید و استاندارد	٤	هر سرور یک عدد
٤۲	آنتن ماهواره ای برای دریافت	جدید و استاندارد	۱	برای کارگاه
٤۳	دستگاه مودم Wi-Max	جدید و استاندارد	٤	هر سرور یک عدد
٤٤	دستگاه مودم Wi-Fi	جدید و استاندارد	٤	هر سرور یک عدد
٤٥	آنتن Transceiver	با زاویه ٤٥ و ۷٥و۹۰و۱۸۰و۳٦۰ درجه		به تعداد لازم
٤٦	کنترل کننده بیومتریک	شناسایی اثر انگشت و چشم و صوت و موارد جدید		به تعداد لازم

توجه :

- تجهیزات برای یک کارگاه به ظرفیت ۱٦ نفر در نظر گرفته شود .

- برگه استاندارد مواد

ردیف	نام	مشخصات فنی و دقیق	تعداد	توضیحات
۱	ماژیک وایت برد	معمولی	۵ عدد	برای کارگاه
۲	کاغذ	معمولی	۱۰۰برگ	برای دونفر
۳	DVD خام	معمولی	٤عدد	برای دونفر
٤	خودکار	معمولی	۱عدد	برای یک نفر
٥	دفترچه یادداشت	۱۰۰برگ معمولی	۱عدد	برای یک نفر
٦	کابل سیار پنج راهه	دارای اتصال زمین	۱عدد	برای هرسیستم
۷	کابل شبکه TP	Cat٦ , Cat۷	-	به میزان کافی
۸	کابل شبکه نوری	SMF, MMF	-	به میزان کافی
۹	کابل کواکسیال	RG٥۹,RG٦,RG٦.۲ و RG٥۸,	-	به میزان کافی
۱۰	انواع سوکت های کابل	Fiber , RJ۱۱,RJ٤٥,BNC و	-	به میزان کافی
۱۱	روپوش کار	کارگاهی	۱ عدد	برای یک نفر

توجه :

- مواد به ازاء یک نفر و یک کارگاه به ظرفیت ۱٦ نفر محاسبه شود .

- برگه استاندارد ابزار

ردیف	نام	مشخصات فنی و دقیق	تعداد	توضیحات
۱	نرم افزار آموزش مربوطه	جدید	۱	برای دونفر
۲	نرم افزار دیکشنری انگلیسی به	بروز و جدید	۱	برای دونفر
۳	سیستم عامل کلاینت ویندوز	بروز و جدید	۱	برای دونفر
٤	سیستم عامل سرور ویندوز	بروز و جدید	٤	برای هر سرور
٥	سیستم عامل کلاینت لینوکس	بروز و جدید	۱	برای دونفر
٦	سیستم عامل سرور لینوکس	بروز و جدید	٤	برای هر سرور
۷	نرم افزارOffice	بروز و جدید	۱	برای دونفر
۸	نرم افزاری Visio	بروز و جدید	۱	برای دونفر
۹	نرم افزار آنتی ویروس مخصوص	بروز و جدید	۱	برای دونفر
۱۰	نرم افزار آنتی ویروس مخصوص	بروز و جدید	۱	برای دونفر
۱۱	نرم افزارهای تخصصی	بروز و جدید	۱	برای دونفر
۱۲	نرم افزارهای تخصصی	بروز و جدید	۱	برای دونفر
۱۳	نرم افزار های امنیتی مخصوص	بروز و جدید	۱	برای دونفر
۱٤	نرم افزار های کنترلی مخصوص	بروز و جدید	۱	برای دونفر
۱٥	نرم افزار های تست مخصوص	بروز و جدید	۱	برای دونفر
۱٦	نرم افزارهای نفوذ مخصوص	بروز و جدید	۱	برای دونفر
۱۷	نرم افزار های امنیتی مخصوص	بروز و جدید	۱	برای دونفر
۱۸	نرم افزار های کنترلی مخصوص	بروز و جدید	۱	برای دونفر
۱۹	نرم افزار های تست مخصوص	بروز و جدید	۱	برای دونفر
۲۰	نرم افزارهای نفوذ مخصوص	بروز و جدید	۱	برای دونفر
۲۱	مجموعه زبانهای برنامه نویسی	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲۲	مجموعه زبانهای برنامه نویسی	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲۳	مجموعه زبانهای برنامه نویسی	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲٤	نرم افزار SQL Server	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲٥	نرم افزار Oracle	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲٦	نرم افزار My Sql	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲۷	تستر شبکه	بروز و جدید	۱	برای دونفر
۲۸	آچار سوکت زدن	بروز و جدید	۱	برای دونفر

۲۹	جعبه ابزار ویژه شبکه	بروز و جدید	۱	برای دونفر
۳۰	Cool Disk	٤گیگابایت یابالاتر	۱	برای یک نفر
۳۱	راهنمای کابل کشی	استاندارد EIA/TIA و انواع جدید	۱	برای کارگاه
۳۲	راهنمای سخت افزار شبکه	استاندارد IEEE ۸۰۲ و انواع جدید	۱	برای کارگاه
۳۳	راهنمای استانداردها و پروتوکل	استاندارد IEEE بروز و جدید	۱	برای کارگاه
۳٤	راهنمای استانداردهای سخت	استاندارد CompTia و سایر	۱	برای کارگاه
۳٥	راهنمای استانداردهای امنیت	استاندارد CompTia و سایر	۱	برای کارگاه
۳٦	راهنمای استانداردهای لینوکس	استاندارد CompTia و سایر	۱	برای کارگاه
۳۷	راهنمای استانداردهای ویندوز	استاندارد Microsoft و سایر	۱	برای کارگاه
۳۸	راهنمای استانداردهای تجهیزات	استاندارد Cisco و سایر	۱	برای کارگاه
۳۹	راهنمای استانداردهای Java	جدید و بروز	۱	برای کارگاه
٤۰	راهنمای استانداردهای Net.	جدید و بروز	۱	برای کارگاه
٤۱	مستندات و راهنمای تجهیزات	جدید و بروز	۱	برای کارگاه
٤۲	مستندات و راهنمای ایمنی و چاه	جدید و بروز	۱	برای کارگاه
٤۳	مستندات و راهنمای نفوذ نرم	جدید و بروز	۱	برای کارگاه

توجه :

- مواد به ازاء یک نفر و یک کارگاه به ظرفیت ۱٦ نفر محاسبه شود .