

بسمه تعالی

معاونت آموزش
دفتر طرح و برنامه های درسی

استاندارد آموزش شایستگی

کارگاہی امنیت شبکه

گروه شغلی فناوری اطلاعات

کد استاندارد شایستگی

۲۵۲۳-۵۳-۰۱۹-۱

تاریخ تدوین : ۹۳/۴/۱



تدوین محتوا و تصویب :

کد استاندارد شایستگی: ۱-۱۹-۰۳-۵۳-۲۵۲۳

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 (World Wide Since) WWS) مالزی- عضو کلوپ مدیران مشاور در خاور میانه
مهندس سارنگ قربانپور 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 کار دانش-
مهندس حسن سلیمانی کارشناس فناوری اطلاعات - مدرس دانشگاه جامع علمی کاربردی- مدیر ارشد سایت شرکت رجا
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 و حرفه 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 حرفه ای کشور ، پلاک ۹۷

تلفن ۹ - ۶۶۵۶۹۹۰۰

دورنگار ۶۶۹۴۴۱۱۷



مشخصات استاندارد شایستگی

عنوان استاندارد شایستگی:	
کارگاهی امنیت شبکه	
شرح استاندارد شایستگی:	
این استاندارد دربر گیرنده و پوشش دهنده شیوه استاندارد مناسب به منظور عملیات کارگاهی 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 ای و سایبری و آشنایی با نهاد های رسیدگی کننده، بررسی و تشخیص روش های غیر مجاز بهره برداری از اطلاعات در سطح شبکه های رایانه ای، 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 ۱ و ۲) 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	: ۶۴ ساعت
- زمان آموزش نظری	: ۱۶ ساعت
- زمان آموزش عملی	: ۴۸ ساعت
بودجه بندی ارزشیابی (به درصد)	
- کتبی:	۲۵%
- عملی:	۶۵%
- اخلاق حرفه ای:	۱۰%
صلاحیت های حرفه ای مربیان:	
لیسانس مهندسی کامپیوتر یا فناوری اطلاعات با حداقل سه سال سابقه کار مرتبط	



استاندارد آموزش
- بر گه‌ی عناصر شایستگی و معیارهای عملکرد

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

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



استاندارد آموزش
برگه تحلیل آموزش

زمان اسمی آموزش: ۱۶ ساعت	دانش:
	<p>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</p>
	<p>چگونگی بررسی و شناسایی امنیت اطلاعات چگونگی بررسی امنیت اطلاعات از دید محرمانگی - جامعیت و صحت چگونگی بررسی و شناسایی مدل های امنیت اطلاعات در سطح شبکه های کامپیوتری چگونگی بررسی و شناسایی 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</p>

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 سایر
 نحوه بررسی سیستم های تشخیص آلودگی و مقابله با آنها

مهارت :

زمان اسمی آموزش: ۴۸ ساعت

تعیین 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 امنیت اطلاعات
 انجام بررسی امنیت اطلاعات از دید محرمانگی – جامعیت و صحت
 انجام بررسی و شناسایی مدل های امنیت اطلاعات در سطح شبکه های کامپیوتری
 انجام بررسی و شناسایی 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 i5 با ۴G Ram یا	۱	برای دو نفر
۲	رایانه مخصوص سرور	سوپر میکرو یا HP چند هسته ای با ۸G Ram یا بالاتر	۴	برای هر ۴ نفر
۳	دیتا پروژکتور و پرده دیتا	ویژه کارگاه	۱	برای کارگاه
۴	میز رایانه کلاینت	مجهز و جدید	۱	برای دو نفر
۵	میز سرور جهت اسمبل	مجهز و جدید	۴	هر سرور یک عدد
۶	صندلی گردان	آموزشی	۱	برای هر نفر
۷	چاپگر لیزری	سیاه و سفید یا رنگی	۱	برای کارگاه
۸	اسکندر	رنگی USB	۱	برای کارگاه
۹	تجهیزات مخابراتی اتصال	خطوط مناسب اتصال و تجهیزات	۱	برای کارگاه
۱۰	وایت برد	حداقل ۲ در ۲.۵ متر	۱	برای کارگاه
۱۱	رک ایستاده	حداقل ۱۸ یونیت	۴	هر سرور یک عدد
۱۲	رک دیواری برای تجهیزات	حداقل ۴ یونیت	۴	هر سرور یک عدد
۱۳	هاب باسیم	حداقل ۱۶ پورت جدید و	۴	هر سرور یک عدد
۱۴	سوییچ باسیم	حداقل ۱۶ پورت جدید و	۴	هر سرور یک عدد
۱۵	روتر باسیم	حداقل ۱۶ پورت جدید و	۴	هر سرور یک عدد
۱۶	بریج باسیم	جدید و استاندارد	۴	هر سرور یک عدد
۱۷	Access Point باسیم	جدید و استاندارد	۴	هر سرور یک عدد
۱۸	فایروال باسیم	سخت افزار جدید و استاندارد	۴	هر سرور یک عدد
۱۹	هاب بی سیم	جدید و استاندارد	۴	هر سرور یک عدد
۲۰	سوییچ بی سیم	جدید و استاندارد	۴	هر سرور یک عدد
۲۱	روتر بی سیم	جدید و استاندارد	۴	هر سرور یک عدد
۲۲	بریج بی سیم	جدید و استاندارد	۴	هر سرور یک عدد
۲۳	تکرار کننده	جدید و استاندارد	۴	هر سرور یک عدد
۲۴	فایروال بی سیم	سخت افزار جدید و استاندارد	۴	هر سرور یک عدد
۲۵	Access Point بی سیم	جدید و استاندارد	۴	هر سرور یک عدد
۲۶	Transceiver - infrared	انعکاسی جدید و استاندارد	۴	هر سرور یک عدد
۲۷	Transceiver - infrared	انعکاسی جدید و استاندارد	۸	هر کلاینت یک

هر سرور یک عدد	۴	جدید و استاندارد	Transceiver - Bluetooth	۲۸
هر کلاینت یک عدد	۸	جدید و استاندارد	Transceiver - Bluetooth	۲۹
هر سرور یک عدد	۴	پخششی جدید و استاندارد	Transceiver - infrared	۳۰
هر کلاینت یک عدد	۸	پخششی جدید و استاندارد	Transceiver - infrared	۳۱
هر سرور یک عدد	۴	P2P جدید و استاندارد	Transceiver - infrared	۳۲
هر کلاینت یک عدد	۸	P2P جدید و استاندارد	Transceiver - infrared	۳۳
هر سرور یک عدد	۴	خشک ، جدید و استاندارد	UPS + Stabilizer	۳۴
هر کلاینت یک عدد	۸	خشک ، جدید و استاندارد	UPS + Stabilizer	۳۵
برای کارگاه	۱	جدید و استاندارد	دستگاه جوش فیوژن و اتصال دهنده کابل‌های	۳۶
هر سیستم یک عدد	۱۲	جدید و استاندارد	کارت شبکه بی سیم	۳۷
هر سیستم یک عدد	۱۲	جدید و استاندارد	کارت شبکه باسیم	۳۸
هر سیستم یک عدد	۱۲	جدید و استاندارد	کارت شبکه نوری	۳۹
هر سرور یک عدد	۴	جدید و استاندارد	آنتن Wi-Fi	۴۰
هر سرور یک عدد	۴	جدید و استاندارد	آنتن Wi-Max	۴۱
برای کارگاه	۱	جدید و استاندارد	آنتن ماهواره ای برای دریافت	۴۲
هر سرور یک عدد	۴	جدید و استاندارد	دستگاه مودم Wi-Max	۴۳
هر سرور یک عدد	۴	جدید و استاندارد	دستگاه مودم Wi-Fi	۴۴
به تعداد لازم		با زاویه ۴۵ و ۷۵ و ۹۰ و ۱۸۰ و ۳۶۰ درجه	آنتن Transceiver	۴۵
به تعداد لازم		شناسایی اثر انگشت و چشم و صوت و موارد جدید	کنترل کننده بیومتریک	۴۶

توجه :

- تجهیزات برای یک کارگاه به ظرفیت ۱۶ 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	۱۰۰ برگ	برای دونفر
۳	DVD خام	معمولی	۴ عدد	برای دونفر
۴	خودکار	معمولی	۱ عدد	برای یک نفر
۵	دفترچه یادداشت	۱۰۰ برگ معمولی	۱ عدد	برای یک نفر
۶	کابل سیار پنج راهه	دارای اتصال زمین	۱ عدد	برای هر سیستم
۷	کابل شبکه TP	Cat۶ , Cat۷	-	به میزان کافی
۸	کابل شبکه نوری	SMF, MMF	-	به میزان کافی
۹	کابل کواکسیال	RG۵۸, RG۵۹, RG۶, RG۶.۲ و	-	به میزان کافی
۱۰	انواع سوکت های کابل	RJ۱۱, RJ۴۵, BNC , Fiber	-	به میزان کافی
۱۱	روپوش کار	کارگاهی	۱ عدد	برای یک نفر

توجه :

- مواد به ازاء یک نفر و یک کارگاه به ظرفیت ۱۶ 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
۴	سیستم عامل سرور ویندوز	بروز و جدید	۴	برای هر سرور
۵	سیستم عامل کلاینت لینوکس	بروز و جدید	۱	برای دونفر
۶	سیستم عامل سرور لینوکس	بروز و جدید	۴	برای هر سرور
۷	نرم افزار Office	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
۱۴	نرم افزار های کنترلی مخصوص	بروز و جدید	۱	برای دونفر
۱۵	نرم افزار های تست مخصوص	بروز و جدید	۱	برای دونفر
۱۶	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
۲۴	نرم افزار SQL Server	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲۵	نرم افزار Oracle	جدید و بروز و متناسب با آموزش	۱	برای دونفر
۲۶	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	۴ گیگابایت یا بالاتر	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
۳۴	راهنمای استانداردهای سخت	استاندارد CompTia و سایر	۱	برای کارگاه
۳۵	راهنمای استانداردهای امنیت	استاندارد CompTia و سایر	۱	برای کارگاه
۳۶	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
۴۰	راهنمای استانداردهای .Net	جدید و بروز	۱	برای کارگاه
۴۱	مستندات و راهنمای تجهیزات	جدید و بروز	۱	برای کارگاه
۴۲	مستندات و راهنمای ایمنی و چاه	جدید و بروز	۱	برای کارگاه
۴۳	مستندات و راهنمای نفوذ نرم	جدید و بروز	۱	برای کارگاه

توجه :

- مواد به ازاء یک نفر و یک کارگاه به ظرفیت ۱۶ نفر محاسبه شود .