دستورالعمل و راهنمای راه‌اندازی مراکز آزمون الکترونیک

معاونت آموزشی

مرکز سنجش آموزش پزشکی -اردیبهشت‌ماه ۱۳۹۸

«فهرست مطالب»

عنوان **شماره صفحه**

مقدمه:

دانشگاه‌ها سرمایه‌ای ملی هستند که همواره توسط افراد و گروه‌های کثیری مورد استفاده قرار می‌گیرند. لذا در نظر گرفتن استانداردهای لازم در طراحی فضاهای مورد نیاز دانشگاهی، می‌تواند کمک فراوانی در امر آموزش و رفاه حال استفاده کنندگان از این نوع خدمات، بخصوص دانشجویان داشته باشد.

برگزاری آزمون، به ویژه در سطوح بالا با تعداد زیادی از داوطلبان، همواره یکی از وقت‌گیرترین، پرهزینه‌ترین و حساس‌ترین موضوعات، برای متولیان این امر بوده است. افراد بسیاری درگیر طراحی سؤال، تایپ و فرمت‌بندی دفترچه آزمون، چاپ و تکثیر، بسته بندی و توزیع دفترچه‌ها قبل از آزمون هستند. همچنین پس از آزمون نیز افرادی درگیر جمع آوری و تصحیح پاسخنامه‌ها، استخراج نتایج و همچنین تحلیل آزمون می شوند. در چنین شرایطی امکان خطا در هریک از مراحل افزایش می‌یابد بنابراین، روش‌های نوین برگزاری آزمون که بتواند تا حد قابل قبولی سرعت، دقت و به ویژه امنیت آزمون‌ها را افزایش بدهد، می‌تواند راه حل مناسبی برای بهبود شرایط کنونی باشد. با استفاده از فناوری‌های پیشرفته و امکانات و زیر ساخت های شبکه‌ای می‌توان در زمان و هزینه صرفه جویی کرد و دقت و سرعت فرایند را بالا برد. سیستم آزمون الکترونیک، شیوه و مدلی است که به صورت ویژه و با لحاظ کردن نکات امنیتی و به روز، این قابلیت را ایجاد کرده است که تعداد کثیری از داوطلبان در آزمون شرکت کرده و بتوان به راحتی آنها را پشتیبانی، مدیریت و کنترل نمود.

از مزایای مخصوص و ویژه‌ی سیستم آزمون الکترونیک می‌توان به قابلیت پشتیبانی از انواع مختلف آزمون از جمله تشریحی و چند گزینه‌ای، سرعت و پردازش بسیار بالا، احتیاج به حداقل امکانات سخت‌افزاری و نرم افزاری برای ارائه سرویس به حداکثر تعداد داوطلبان شرکت کننده در آزمون، فضای امنیتی بسیار بالا در برگزاری آزمون و احتمال کمترین درصد تخلف و خطا، قابلیت دیدن کارنامه نتایج و پاسخ نامه بلافاصله پس از اتمام آزمون اشاره نمود.

به منظور وحدت رویه، دستورالعمل و راهنمای برگزاری آزمون‌های الکترونیکی براساس سیاست‌های مرکز سنجش پزشکی، تهیه و تدوین گردیده است.

❖ تعاریف:

۱) **مرکز سنجش آموزش پزشکی:** در سال ۱۳۶۴ به منظور استفاده مطلوب و هماهنگ از امکانات پزشکی کشور و در جهت تأمین و تعمیم بهداشت و درمان و بهزیستی و آموزش و پژوهش، وزارت بهداشت، درمان و آموزش پزشکی تشکیل شد. وظایف و تشکیلات این وزارتخانه در سال ۱۳۶۷ به تصویب مجلس شورای اسلامی رسید و در نتیجه دانشگاه‌های علوم پزشکی و مؤسسات آموزش عالی و بیمارستان‌های آموزشی از وزارت علوم، تحقیقات و فناوری جدا و به این وزارتخانه واگذار گردید. از همان زمان آزمون‌های مختلف توسط واحد آزمون‌سازی برگزار گردید. از سال ۱۳۸۴ مرکز سنجش آموزش پزشکی به طور رسمی عهده‌دار برگزاری آزمون های مختلف نظیر کارشناسی ارشد، دکتری تخصصی(Ph.D)، دستیاری تخصصی پزشکی گردید.

۲) **مرکز برگزار کننده آزمون الکترونیک:** که در این دستورالعمل به اختصار مرکز آزمون نامیده می‌شود، مرکزی است واجد شرایط برگزاری آزمون الکترونیکی که دارای فضایی کافی، اتاق سرور اختصاصی، سالن انتظار و ایستگاه‌های کاری آزمون‌گیری و امکانات جانبی می‌باشد.

۳) **مرکز سنجش (الکترونیکی):** به واحدی اجرایی گفته می‌شود که با توجه به شرایط فیزیکی و تجهیزات رایانه‌ای اعلام شده از طرف مرکز سنجش آموزش پزشکی وزارت بهداشت درمان و آموزش پزشکی، امکان اجرا و مدیریت آزمون‌های کتبی و عملی علوم پزشکی را به صورت الکترونیکی دارد. این مرکز زیر نظر معاونت آموزشی دانشگاه علوم پزشکی فعالیت می‌نماید.

۴) **داوطلب آزمون الکترونیکی:** فردی است که حائز شرایط شرکت در آزمون بوده که بر اساس میل و رغبت خود متقاضی شرکت در آزمون الکترونیکی است. برای تعیین صلاحیت، ارزیابی و سنجش وی از ابزارهای رایانه‌ای استفاده می‌شود.

۵) **سالن انتظار:** مکانی در مرکز آزمون است که آزمون دهندگان قبل از مستقر شدن در سالن آزمون، وارد آنجا شده و راهنمایی‌های لازم در خصوص فرایند برگزاری آزمون الکترونیکی، به آنها ارائه می‌شود.

۶) **سالن برگزاری آزمون الکترونیکی:** محل اصلی برگزاری آزمون می‌باشد. این سالن برای استقرار داوطلبان، عوامل اجرایی و تجهیزات مورد نیاز جهت آزمون الکترونیکی در فرایند آزمون مورد نیاز است.

۷) **ایستگاه کاری:** به محل استقرار آزمون دهندگان در سالن آزمون الکترونیکی گفته می‌شود. هر ایستگاه کاری از یک میز رایانه‌ای پارتیشن دار، صندلی و یک سیستم رایانه (متصل به سرور مرکز آزمون) و سایر دستگاه‌های جانبی مورد نیاز، تشکیل شده است.

۸) **اتاق سرور:** مکانی در محل برگزاری آزمون است که برای استقرار تجهیزات رایانه‌ای از قبیل سرور و ملزومات شبکه در نظر گرفته می‌شود. از این اتاق جهت مدیریت نرم افزار آزمون الکترونیکی استفاده می‌شود.

۹) **اتاق مانیتورینگ** : مکانی در محل برگزاری آزمون است که برای استقرار ناظر (ناظرین) و تجهیزات مورد نیاز جهت نظارت بر روند اجرای آزمون و ذخیره سازی اطلاعات صوتی و تصویری آزمون دهندگان در نظر گرفته می شود.

۱۰) **سیستم صوتی مرکزی:** به سیستم صوتی‌ای نصب شده در مرکز آزمون الکترونیک گفته می‌شود که جهت اطلاع رسانی به داوطلبان قبل، حین و بعد از آزمون کاربرد دارد.

۱۱) **عوامل اجرایی:** به افرادی گفته می‌شود که بر فرایند برگزاری آزمون نظارت و کنترل داشته و در برابر وظایف تعیین شده که به تفصیل در بخش شرح وظایف همین دستور العمل بیان خواهد شد، مسؤلیت دارند.

۱۲) **مسؤل فنی مرکز سنجش (الکترونیک):** فردی است که کلیه‌ی امور فنی رایانه‌ای و شبکه مرکز سنجش را به لحاظ سخت افزاری و نرم افزاری بر عهده دارد.

❖ مشخصات مرکز آزمون الکترونیک:

محل برگزاری آزمون الکترونیک، متشکل از بخش‌های زیر می‌باشد.

۱- سالن انتظار
۲- سالن (سالن‌های برگزاری آزمون)
۳- ایستگاه کاری
۴- اتاق سرور
۵- سیستم صوتی مرکزی
۶- اتاق مانیتورینگ

۱. سالن انتظار

در این سالن برای اطلاع رسانی به آزمون دهندگان، باید به تعداد کافی تابلوهای راهنما و اعلانات در فضای مناسب نصب شده باشد، بطوریکه موقعیت سالن‌ها و شماره‌ی صندلی‌ها را نشان داده و آزمون دهندگان را در رسیدن به محل سالن آزمون راهنمایی کند. حداقل فضای مورد نیاز برای سالن انتظار به‌طور تقریبی برای هر چهار نفر، یک متر مربع می‌باشد. وجود صندلی، ساعت دیواری، نور کافی، تهویه مطبوع، آبخوری، سرویس بهداشتی و ...در این مکان علاوه بر کاهش استرس داوطلب، می‌تواند نقش مؤثری در تسهیل روند آزمون داشته باشد.

در این سالن می‌توان راهنمایی و آموزش‌های لازم را جهت اجرای فرایند آزمون به داوطلبان ارائه نمود. همچنین وجود سالن انتظار، می‌تواند تجمع افراد در پشت درب مرکز آزمون در زمان کنترل و شناسایی داوطلبان را کاهش دهد.

جهت انجام کارهای اداری آزمون، بهتر است اتاقی مجزا و مجهز به سیستم‌های ارتباطی(اینترنت، تلفن و نمابر)، کپی، رایانه، اسکنر و چاپگر در نزدیکی سالن انتظار در نظر گرفته شود. محل استقرار این مکان باید به گونه‌ای باشد تا صدای آن در هنگام برگزاری، موجب برهم زدن نظم آزمون نگردد. در هر صورت این اتاق باید خارج از سالن یا سالن‌های آزمون و در مرکز آزمون قرار گرفته باشد.

۲. سالن یا سالن‌های آزمون الکترونیک

۲-۱- فضای فیزیکی

مد نظر قرار دادن شرایط فیزیکی هر سالن تأثیر بسزایی در استفاده مطلوب از آن دارد. نظر به حساسیت سالن آزمون الکترونیک و بر اساس استانداردها باید راهروها و سالن‌های آزمون مجهز به دوربین مدار بسته باشد. پوشش دوربین‌ها باید به نحوی باشد که هیچ نقطه کوری به ویژه در سالن‌های آزمون الکترونیکی وجود نداشته باشد. با توجه به اینکه در حین اجرای فرآیند آزمون، داوطلب به هیچ عنوان حق خروج از سالن آزمون را ندارد، وجود سرویس‌های بهداشتی در کلیه سالن‌ها اجباری بوده و چنانچه سالن‌های آزمون در طبقات متفاوت و بیش از یک طبقه باشد، وجود سرویس بهداشتی در هر طبقه لازم و ضروری است.

۲-۲- چیدمان ایستگاه‌های کاری

چیدمان ایستگاه‌های کاری بایستی به گونه‌ای باشد تا ضمن استفاده از حداکثر فضای سالن، داوطلب هیچگونه دیدی به مانیتور سایر داوطلبان نداشته باشد و مراقبان ضمن امکان تردد راحت در بین ایستگاه‌ها، اشراف کاملی به همه داوطلبان داشته باشند.

فاصله هر داوطلب با داوطلب سمت راست یا چپ (ترجیحاً یک متر) باید به نحوی باشد که ضمن فراهم کردن فضای مناسب و راحت، با ایجاد دیوار حائل بین نمایشگر داوطلبان، باعث افزایش اعتبار آزمون گردد.

۲-۳- تجهیزات شبکه

کابل کشی شبکه و برق مورد نیاز، از شاهراه‌های حیاتی مرکز آزمون بوده و از الزامات اتصال سیستم کاربر به سرور آزمون می‌باشد. لذا رعایت استانداردهای کابل کشی ساختاریافته در این خصوص لازم و اجباری است. این کابل‌کشی باید به گونه‌ای باشد که داکت‌ها و کابل‌کشی شبکه و برق به هیچ وجه در دسترس همگان نباشد. بهتر است بیش از نیاز فعلی پریز شبکه یا Outlet در نظر گرفته شود. در کابل کشی شبکه، حتماً وجود میدان‌های مغناطیسی و تأثیر آن بر سرعت و عملکرد شبکه، مد نظر قرار داده شود.

۲-۴- امکانات فیزیکی

سالن باید داری تهویه هوای مطبوع، سیستم گرمایش و سرمایش مناسب (باتوجه به شرایط جغرافیایی منطقه) بوده و از نور کافی برخوردار باشد. نور خورشید در سالن به گونه‌ای نباشد که داوطلب در مشاهده صفحه نمایش خود دچار مشکل شود. با توجه به این موضوع که زمان در حین برگزاری آزمون از اهمیت بسزایی برخوردار است، وجود ساعت دیواری در معرض دید همه داوطلبان الزامی است. سیستم صوتی که جهت راهنمایی و اطلاع رسانی در سالن نصب

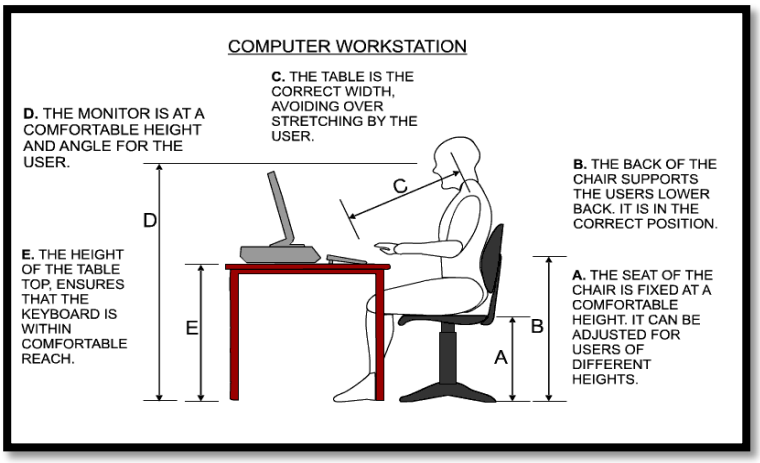
گریده است، به گونه ای نباشد تا موجب آزار برخی از داوطلبان گردد و تعبیه آن به صورتی باشد تا صدا به طور کامل و واضح به همه داوطلبان برسد.

ضروری است تا سیستم روشنایی سالن مجهز به برق اضطراری بوده تا در صورت قطع برق، داوطلبان در ادامه فرایند آزمون دچار مشکل نشوند.

همچنین سالن باید دارای سیستم اطفاء حریق و کمک‌های اولیه مناسب باشد. برای اطلاع رسانی به آزمون‌دهندگان، باید به تعداد کافی تابلوهای راهنما و اعلانات، تابلوهای هشدار، اطلاع رسانی و ضوابط برگزاری آزمون در فضای مناسب، نصب شده باشد.

در محل سالن آزمون، استفاده از وسایل ارتباطی از جمله تلفن ثابت، تلفن همراه، بی‌سیم، پیجر و ... اکیداً ممنوع است.

۳. ایستگاه آزمون:



چیدمان راحت و حرفه‌ای قطعات فیزیکی رایانه متناسب با اصول ارگونومی، اولین رهاورد بهره‌گیری از یک میز کار اختصاصی است. البته علاوه بر چیدمان صحیح، یک میز مناسب از مشکلات ناشی از حرکت ناگهانی قطعات و حتی خرابی احتمالی کامپیوتر جلوگیری می‌کند.

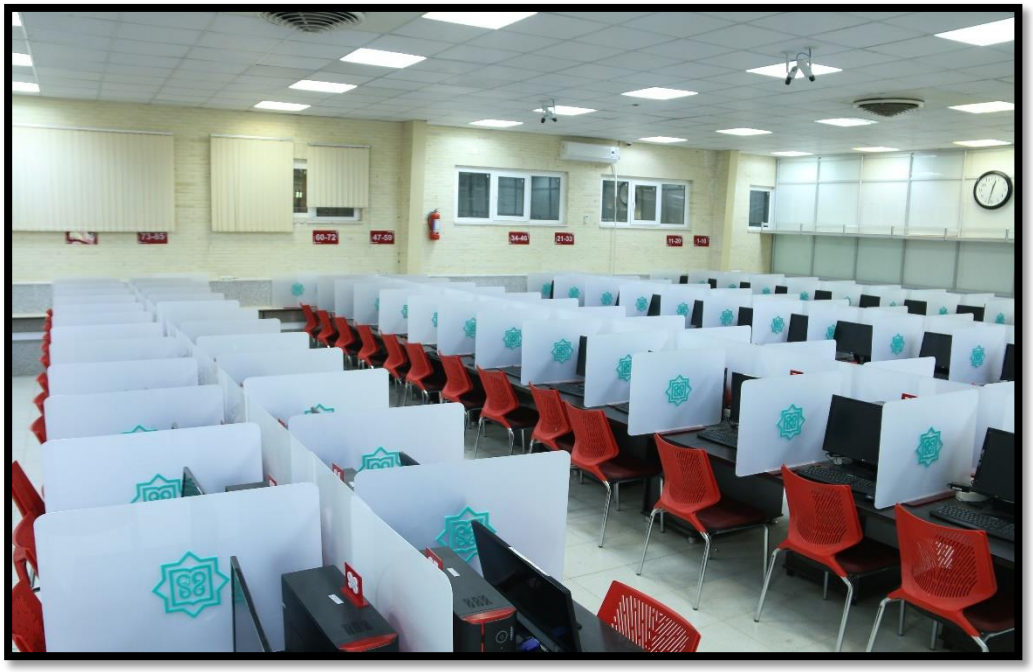
محل استقرار آزمون دهندگان در سالن آزمون الکترونیکی از یک میز رایانه‌ای پارتیشن‌دار، صندلی و یک دستگاه سیستم رایانه متصل به سرور مرکز آزمون تشکیل شده است. این اتصال باید در یک شبکه LAN مجزا (به صورت فیزیکی کاملاً جدا از دیگر شبکه‌ها) جهت برقراری ارتباط بین رایانه‌ها و سرور آزمون باشد و داکت‌ها و کابل کشی شبکه و برق به هیچ وجه در دسترس عموم نباشد. اتصال ایستگاه کاری به پریز برق سالن آزمون کاملا محکم بوده و در محل تردد و استقرار داوطلب قرار نگرفته باشد. برق مورد استفاده ایستگاه کاری حتماً به UPS متصل باشد. کابل‌های شبکه حتماً درون داکت قرار گرفته باشد. چیدمان صحیح میزهای ایستگاه کاری باعث تردد راحت تر عوامل اجرایی بوده و همچنین این موضوع باعث جلوگیری از بر هم خوردن تمرکز داوطلب خواهد شد.

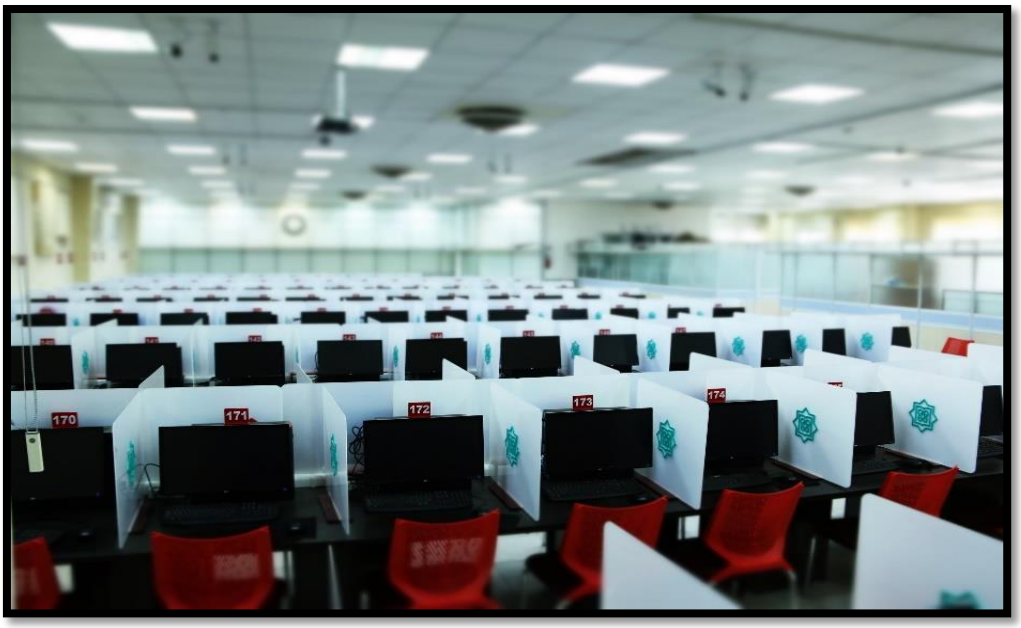
میز کاری محل استقرار آزمون‌دهندگان در سالن آزمون است که باید دارای مشخصات زیر باشد:

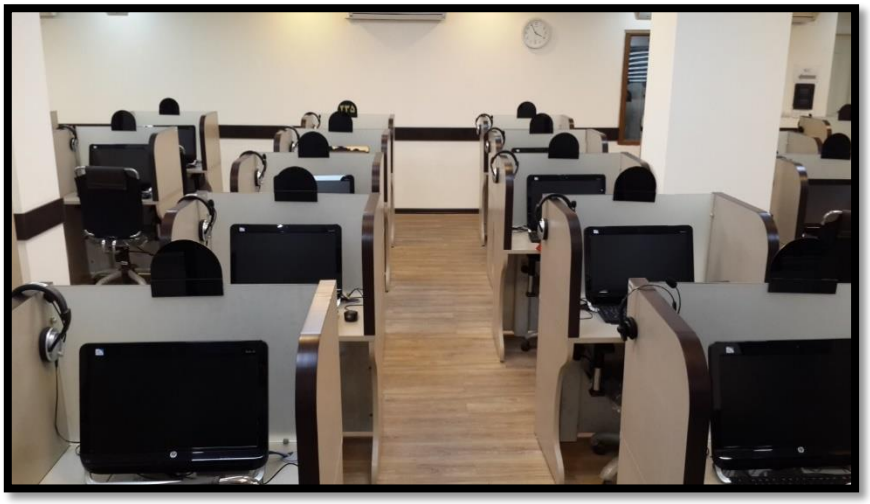
- یک میز پارتیشن‌دار با حداقل ابعاد ۸۰*۶۰ سانتی‌متر
- فاصله سطح میز از کف سالن باید ۷۰ سانتی‌متر باشد.
- سه دیواره پارتیشن برای هر ایستگاه کاری در نظر گرفته شود. ارتفاع هر یک از دیواره‌های پارتیشن از سطح میز باید ۵۰ سانتی‌متر باشد. توصیه می‌شود پارتیشن متحرک باشد.
- یک عدد صندلی متحرک، دوار و با پایه چرخ‌دار، بدون دسته (ارتفاع صندلی براساس قد قابل تغییر باشد)
- حداقل یک عدد پریز برق
- حداقل یک عدد پریز شبکه

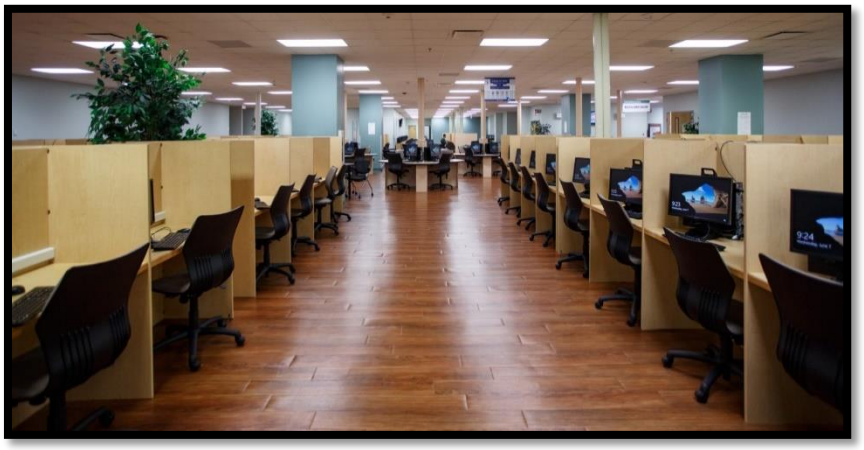
نحوه چینش میزهای رایانه در سالن‌های کم عرض و عریض متفاوت می‌باشد. در سالن‌هایی با عرض کم می‌توان ایستگاه‌های کاری را رو به دیوار قرار داد و در سالن های عریض، می توان ایستگاه‌های کاری را در چند ردیف طولی و پشت سر هم چید طوریکه فاصله هر ردیف از ردیف دیگر حداقل ۱ متر باشد. همچنین هر ردیف فاصله حداقل یک متری از ایستگاه‌های کاری جلوی یا پشتی خود داشته باشد. ضروری است تا چیدمان به گونه‌ای باشد تا به هیچ عنوان داوطلب به غیر از صفحه مانیتور خود صفحه مانیتور دیگری را نبیند. تصویر چند چیدمان نمونه در تصاویر زیر آورده شده است.

«شکل چیدمان متفاوت با توجه به فضای فیزیکی و امکانات موجود»




170
171
172
173
174





۳-۱- مشخصات قابل قبول رایانه‌های آزمون:

۳-۱-۱- سیستم‌های دارای پردازشگر

مشخصات این سیستم‌ها به شرح ذیل می‌باشد.

ردیف	تجهیزات رایانه
۱	CPU: Intel core i3 Mother Board: mini ATX core i3 support
۲	RAM :4G DDR4
۳	HDD : 120G ssd or m2
۴	Network Adapter speed 1000Mbps
۵	Keyboard (simple)
۶	Mouse 2 keys (without backward or forward keys)
۷	Monitor IPS panel 20 or 22 inch
۸	هدفون سیم دار با کیفیت قابل قبول

***تذکر۱:** سیستم‌های کاری به هیچ عنوان به تجهیزات بی سیم مانند بلوتوث[۱] و وای فای[۲] مجهز نباشد.

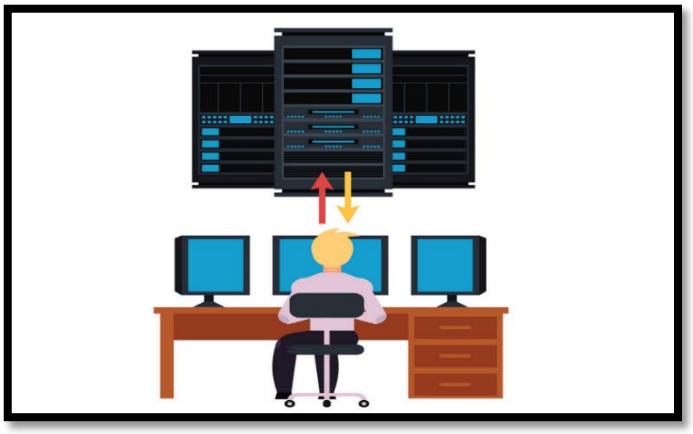
***تذکر۲:** غیرفعال نمودن پورت‌های USB و CD/DVD ROM لازم و اجباری می‌باشد.

۳-۱-۲- سیستم‌های بدون پردازشگر

امروزه استفاده از سیستم‌های رایانش ابری همچون زیروکلاینت، دسترسی به منابع فناوری اطلاعات در زمان تقاضا و بر اساس میزان تقاضای کاربر به گونه‌ای انعطاف‌پذیر و از راه شبکه به کاربر را فراهم می‌آورد. مشخصات قابل قبول در ایستگاه کاری در این سیستم‌ها به شرح جدول ذیل می‌باشد:

ردیف	تجهیزات رایانه
۱	زیرو کلاینت با کیفیت تصویر قابل قبول
۲	Keyboard (simple)
۳	Mouse 2 keys (without backward or forward keys)
۴	Monitor IPS panel 20 or 22 inch
مشخصات سرور مورد نیاز به ازای هر ۵۰ایستگاه	
۵	Server DL380 GEN9 CPU:intel XEON e52600 v4 RAM:128G HDD:4*1TB

[۱] Bluetooth
[۲] Wi-Fi



۴. اتاق سرور[۳]:

سرور قلب تپنده هر شبکه رایانه‌ای است. بطوریکه هرگونه اشکال در عملکرد آن، باعث اختلال در سیستم‌ها شده و خسارت فراوانی را در پی خواهد داشت. که این خسارات در برخی موارد جبران ناپذیر می‌باشد. انتخاب تجهیزات مناسب اتاق سرور یکی از راهکارهای کنترل کارکرد صحیح و بهینه این قلب تپنده می‌باشد. یکی از مهمترین عوامل در عملکرد صحیح این تجهیزات، وجود شرایط مناسب محیطی همچون دما، رطوبت و ولتاژ مناسب است. نکته مهم دیگر وضعیت امنیت و ایمنی اتاق سرور می‌باشد که آن را در مقابل دستبرد، حریق (آتش سوزی) و سایر خطرات احتمالی، حفظ نماید.

در مراکز سنجش الکترونیک، اتاق سرور مرکز آزمون، مکانی است در سالن برگزاری آزمون که برای استقرار تجهیزات رایانه‌ای از قبیل سرور، سوییچ و ملزومات شبکه در نظر گرفته می‌شود. از این اتاق جهت مدیریت نرم افزار آزمون الکترونیک، استفاده می‌شود. این اتاق باید تا جای ممکن در نزدیک‌ترین موقعیت به سالن یا سالن‌های آزمون باشد. همچنین در آزمون های الکترونیک، کلیه عملیات مربوط به فرایند آزمون از قبیل ورود داوطلب به صفحه آزمون، مشاهده و پاسخ به سؤال، کنترل زمان و ثبت نتایج آزمون، و .... در سرور آزمون صورت می‌پذیرد. لذا توجه ویژه به اتاق سرور دوچندان بوده و به تبع امری اجتناب ناپذیر خواهد بود.

لازم است تا کلیه تجهیزات شبکه از قبیل سرور، ایستگاه‌های کاری، سوییچ ها و کابل های شبکه به صورت فیزیکی از دیگر شبکه‌ها جدا درنظر گرفته شود. توجه به این نکته ضروری است که استفاده از سایر سرورهای دانشگاه در مرکز آزمون، اکیداً ممنوع بوده و سرور آزمون باید بصورت فیزیکی در مرکز آزمون، قرار داشته باشد.

اندازه اتاق نسبت به سخت افزارها و تجهیزات موجود، با حداقل ارتفاع ۲/۵ متر در نظرگرفته شود. توجه به سیستم سرمایشی اتاق سرور و همچنین رویه های امنیتی از جمله سیستم کنترل تردد، نصب دوربین مداربسته، سیستم اعلام و اطفاء حریق لازم و ضروری است.

---

[۳] Server Room

۴ –۱–UPS اتاق سرور

یکی از دستگاه‌های اتاق سرور UPS است،که باعث عملکرد نرمال سرورها در زمان قطع و وصل شدن جریان برق خواهد شد. در اتاق‌های سروری که بدون UPS باشند، قطعاً با قطع و وصل شدن برق، سرورها از کار افتاده یا دچار آسیب‌هایی می‌شوند. لذا به وسیله UPS می‌توان از بروز این مشکلات جلوگیری کرد. لذا لازم است با توجه به میزان مصرفی تجهیزات رایانه و شبکه‌ای موجود، نسبت به راه‌اندازی UPS مناسب اقدام گردد.

❖ **تذکر بسیار مهم:** اتصال کلیه دستگاه‌های الکترونیکی مستقر در اتاق سرور، اعم از سرور و سوییچ‌ها به UPS، اجباری است.

۴–۲ – دسترسی فیزیکی

دسترسی فیزیکی به اتاق سرور باید تنها به چند نفر که اجازه دسترسی را به طور قانونی دارند، محدود باشد. استفاده از کارت خوان یا قفل الکترونیک برای اجازه دسترسی نسبت به کلیدهای مرسوم، پیشنهاد می‌شود. لیست افراد مجاز برای ورود باید حداقل توسط حراست تأیید گردد. استفاده از دوربین های مدار بسته برای کنترل، ثبت ورود و خروج و کار در این فضا پیشنهاد می شود. همچنین باید ثبت زمان ورود، زمان خروج، هدف از دسترسی فیزیکی توسط بازدید کنندگان یا پرسنل مجاز مشخص شود.

۴–۳– مشخصات سرور

مشخصات قابل قبول سرور جهت سرویس دهی تا هزار داوطلب به شرح جدول ذیل می‌باشد.

ردیف	تجهیزات
۱	hp proliant dl380 gen9 (CPU: Intel Xeon E5-2600)
۲	RAM: 64 GDDR4
۳	HDD: 1TB*4

❖ **تذکر بسیار مهم:** حتماً برروی سرور آنتی ویروس با آپدیت معتبر و به روز نصب شده باشد.

۴–۴– سوییچ شبکه

سوئیچ شبکه با قابلیت کانفیگ به ازای هر ۴۰ ایستگاه کاری، یک عدد سوئیچ ۴۸ پورت مورد نیاز است (جهت ارتقاء و استفاده در آینده، ترجیحاً سوییچ PoE استفاده گردد). در کابل‌کشی کابل و داکت استاندارد، به کار گرفته شود.

۴–۵– چک لیست امنیتی ویندوز سرور

یکی از مهمترین مسائلی که در شبکه مطرح است و به آن توجه کمتری می شود امنیت در لایه سیستم عامل و به ویژه سیستم عامل ویندوز سرور است، فرایند امنیتی که برای امن سازی سرورهای ویندوزی و لینوکسی انجام می شود و درجه امنیتی آنها را بالا می برد به عنوان Server Hardening شناخته می شود. نصب و اجرای چک لیست‌های زیر در اتاق سرور لازم و ضروری می‌باشد.

چک لیست امنیتی وب سرور IIS

۱- به هیچ عنوان سروری که بصورت کامل فرآیند Hardening بر روی آن انجام نشده است را به اینترنت متصل نکنید.

۲- سرور را در محل فیزیکی امن قرار بدهید، امنیت فیزیکی از اولین مواردی است که در حوزه امنیت باید رعایت شود.

۳- به هیچ عنوان وب سرور IIS را بر روی Domain Controller نصب نکنید.

۴- بر روی وب سرور IIS هرگز پرینتر نصب نکنید.

۵- بر روی سرور دو عدد کارت شبکه بگذارید، یکی برای مدیریت سرور و دیگری برای کاربران.

۶- حتماً Service Pack ها، Patch ها و البته Hotfix های لازم را بر روی سیستم عامل سرور نصب کنید.

۷- ابزار IIS Lockdown را بر روی سرور وب اجرا کنید (در IIS های قدیمی و ویندوزهای سرور قدیمی)

۸- ابزار امنیتی URLScan را بر روی وب سرور نصب، اجرا و پیکربندی کنید.

۹- حتماً برای Remote Desktop از Encryption مناسب استفاده کنید.

۱۰-حتماً برای Remote Desktop قابلیت های Account Lockout و Session Timeout را قرار دهید.

۱۱-هرگونه سرویس بلااستفاده بر روی سیستم عامل ویندوز را غیرفعال کنید.

۱۲-مطمئن شوید که همگی سرویس ها با حداقل دسترسی کاربری اجرا می‌شوند.

۱۳-اگر به سرویس های SMTP،FTP و NNTP نیازی ندارید، آنها را غیرفعال یا حذف کنید.

۱۴-سرویس Telnet را حتماً غیرفعال و از روی سیستم عامل حذف کنید.

۱۵-اگر سرویس وضعیت ASP.NET یا ASP.NET State Service توسط Application های شما استفاده نمی‌شود آن را غیرفعال کنید.

۱۶-اگر از WebDAV استفاده نمی کنید یا مطمئن هستید Application های شما از آن استفاده نمی کنند آن را غیرفعال کنید.

۱۷-اگر از WebDAV استفاده می‌کنید حتماً پارامترهای امنیتی آن را رعایت کنید.

۱۸-قسمت Data Access Components را فقط در صورت نیاز نصب کنید. در غیر اینصورت آن را حذف کنید.

۱۹-قسمت MS Index Server را فقط در صورت نیاز نصب کنید و اگر نیازی نیست نصب نکنید.

۲۰-گزینه HTML Version از قسمت Internet Service Manager را اصلاً فعال یا نصب نکنید.

۲۱-قسمت MS FrontPage Server extensions را فقط در صورت نیاز نصب کنید در غیر اینصورت حذف کنید.

۲۲-فرآیند Hardening را برای TCP/IP Stack هم انجام دهید.

۲۳-Policy های مربوط به Recycle Bin و Paging File System را (به تناسب سرور)مجدداً پیکربندی کنید.

۲۴-تنظیمات امنیتی CMOS را انجام دهید.

۲۵-امنیت فیزیکی مربوط به CD-ROM و USB Drive ها و ... را فراهم کنید.

چک لیست امنیتی Account ها یا حساب های کاربری

۱- هرگونه حساب کاربری اضافه و بلااستفاده را از روی سرور حذف کنید.
۲- حساب کاربری Guest را غیرفعال کنید.
۳- نام کاربر Administrator را عوض کنید و یک پسورد قوی برای آن انتخاب کنید.
۴- حساب کاربری IUSR_MACHINE را در صورتیکه Application ای از آن استفاده نمی‌کنید غیرفعال کنید.
۵- یک حساب کاربری با دسترسی محدود برای anonymous account ها ایجاد کنید. البته در صورتیکه این سرویس را نیاز دارید.
۶- به هیچ عنوان به کاربر anonymous دسترسی بصورت write بر روی محتوای دایرکتوری ها و اجرای دستورات بر روی سرور ندهید.
۷- اگر بر روی سرور شما چندین Web Application وجود دارد، برای هر کدام کاربر anonymous جداگانه‌ای تعریف کنید.
۸- دسترسی‌های حساب کاربری process های ASP.NET را با کمترین سطح دسترسی ممکن تعریف کنید.
۹- گزینه قبل زمانی کاربردی است که شما از اکانت پیش‌فرضی که برای سرویس ASP.NET تعریف شده است استفاده نمی‌کنید.
۱۰-از یک Password Policy قوی برای کلیه اکانت‌های موجود بر روی سرور، استفاده کنید.
۱۱-دسترسی Remote را به حداقل ممکن برسانید، گروه Everyone را از قسمت Access this computer from network حذف کنید.
۱۲-برای هر کدام از Administrator های سرور یک اکانت جداگانه تعریف کنید و اکانت مشترک ایجاد نکنید.
۱۳-Null Session را غیرفعال کنید یا به بیانی دیگر Anonymous Logon را غیرفعال کنید.
۱۴-برای تفکیک کردن اکانتها و کاربردهایشان حتما بایستی تأییده دریافت شود (هر شخص نتواند به شخص دیگری دسترسی بدهد)
۱۵-در گروه Administrators بیشتر از دو کاربر تعریف شده، نداشته باشید.
۱۶-فقط اجازه Logon بصورت Local را بدهید، یا برای Remote Desktop حتما از رمزنگاری استفاده کنید.

چک لیست امنیتی فایل ها و پوشه ها

۱- همیشه چند عدد پارتیشن بر روی هارد دیسک ایجاد کنید.
۲- هیچگاه Home Directory مربوط به وب سرور را در پارتیشن سیستم عامل قرار ندهید.
۳- فایل‌ها و پوشه‌های خود را، بر روی پارتیشن‌هایی که فایل سیستم آن NTFS است قرار دهید.
۴- محتویات هر وب سایت را در پوشه‌ای غیر از Home Directory وب سرور قرار دهید که NTFS هم باشد.
۵- همیشه یک وب سایت جدید ایجاد کنید و وب سایت پیش فرض یا Default Site را، غیرفعال کنید.
۶- از وب سرور بصورت متناوب لاگ برداری کنید و لاگ‌ها را مرتب بررسی کنید.

۷- فایل های Log وب سرور را در پارتیشنی غیر از پارتیشنی که محتویات وب سایت در آن قرار دارند قرار دهید (NTFS باشد).
۸- دسترسی گروه Anonymous و Everyone به پوشه‌های system32 و پوشه وب سایت ها را محدود کنید.
۹- مطمئن شوید که دایرکتوری ریشه یا Root Directory وب سرور، به کاربران گروه Anonymous به هیچ عنوان دسترسی نداده باشد.
۱۰-مطمئن شوید که دایرکتوری هایی که شامل محتویات اطلاعاتی وب سرور هستند، به کاربران گروه Anonymous به هیچ عنوان دسترسی نداده باشند.
۱۱-در هر دو مورد گذشته ترجیحاً از گزینه Deny برای Access Control Entry های Permission ها استفاده کنید.
۱۲-قابلیت Remote IIS Administration یا Remote WWW Administration را به همراه سرویس آن غیرفعال و یا حذف کنید.
۱۳-تمامی ابزارهای Resource Kit به همراه SDK ها را از روی وب سرور حذف کنید.
۱۴-تمامی Sample Application ها یا برنامه‌های پیش‌فرض مثل وب سایت پیش‌فرض IIS را حذف کنید. (از جمله صفحات Help)
۱۵-آدرس IP را از Header حذف کنید. (برای جلوگیری از شناسایی محل یا Content Location)

چک لیست امنیتی Share های شبکه

۱- تمامی Shareهای بلااستفاده از جمله Administrative share ها را از بین ببرید.
۲- حتماً دسترسی‌ها را به افراد مجاز دهید و هیچگاه گروه everyone را در لیست دسترسی‌ها قرار ندهید.
۳- توجه کنید که سیستم های مانیتورینگی مثل SCOM و SCCM از سری System Center با Administrative Share ها کار می‌کنند.
۴- فقط پورت‌های مورد استفاده در File and Printer Sharing را در فایروال باز کنید.
۵- دسترسی به شبکه اینترنت را فقط از طریق پورت‌های ۸۰ و در صورت نیاز ۴۴۳ مجاز کنید.
۶- حتماً استفاده از اینترنت را محدود کنید و فقط از پروتکل های امنی چون SSL برای دسترسی به اینترنت استفاده کنید.
۷- اگر تعداد استفاده کنندگان از Share ها مشخص است، محدودیت Concurrent Connections بر روی Share ها بگذارید.

چک لیست امنیتی Registry

۱- سرویس Remote Registry را غیرفعال کنید و یا دسترسی به آن را محدود کنید.
۲- برای سرورهای Standalone فایل SAM را حتماً امن کنید و در تنظیمات رجیستری NoLMHash را فعال کنید.
۳- حتماً قابلیت‌های Auditing و Logging را بر روی سرورها، فعال کنید.
۴- حتماً Failed Logon Attempts را Audit کنید.

۵- محل Log فایل های IIS را تغییر دهید.
۶- هر چند وقت یکبار Log ها را آرشیو و تجزیه و تحلیل کنید. (حدالمقدور قسمت‌های امنیتی لاگ ها را)
۷- حداکثر اندازه لاگ فایل را تعریف کنید.
۸- دسترسی به فایل Metabase.bin را همیشه Audit کنید.
۹- تنظیمات IIS را به گونه‌ای انجام دهید که قالب W3C Extended Log File نیز بازرسی یا Audit شود.
۱۰-بصورت متناوب از رجیستری خودتان Backup تهیه کنید.

چک لیست امنیتی Site ها و Virtual Directory ها

۱- هیچگاه وب سایت‌ها را بر روی پارتیشن سیستم ایجاد نکنید.
۲- تنظیمات Parent Path را غیرفعال کنید.
۳- Virtual Directory های خطرناکی مثل IISSamples و IISAdmin و IISHelp و Scripts را حذف کنید.
۴- Virtual Directory مربوط به MSADC را حذف کنید.
۵- Virtual Directory به نام IIS Internet Printing را حذف کنید.
۶- مطمئن شوید که Certificate های سرور معتبر و به روز هستند.
۷- از هر Certificate فقط برای کاری که برای آن تعریف شده است استفاده کنید.
۸- مطمئن شوید که Public Key مربوط به Certificate ای که دریافت کرده‌اید معتبر است.
۹- مطمئن شوید که Certificate مورد استفاده شما Revoke نشده باشد.
۱۰-ISAPI Filter های بلااستفاده را از روی سرور حذف کنید.

۵– سیستم صوتی مرکزی: نصب سیستم صوتی مرکزی جهت اطلاع رسانی به داوطلبین در سالن های انتظار، آزمون و راهروها الزامی می‌باشد.

۶–اتاق مانیتورینگ

اتاق مانیتورینگ که مجهز به تجهیزات مورد نیاز جهت نظارت بر روند اجرای آزمون و ذخیره سازی اطلاعات صوتی و تصویری آزمون دهندگان است، باید نزدیکترین محل به سالن آزمون باشد. این اتاق باید به برق UPS مرکز آزمون الکترونیک متصل بوده و در زمان آزمون (حین ضبط آنلاین کلیه تصاویر) توسط اپراتور مانیتورینگ کنترل گردد تا درصورت مشاهده مورد خاص موضوع به مسؤلین ذیربط انتقال داده شود. لازم است در راه اندازی اتاق مانیتورینگ از دستورالعمل حراست استفاده شود.