

باسمه تعالی

شرح وظایف
واحد فناوری اطلاعات
دانشگاه علوم پزشکی اصفهان

ویرایش اول

پاییز ۱۴۰۱

فهرست

پیش نیازها:

- ۱- اجرای کلیه این شرح وظایف به صورت مستقیم توسط کارشناس یا مسئول فناوری اطلاعات هر واحد منوط به وجود تعداد کارشناس متناسب با حجم کار، تعداد و تنوع سخت افزار و نرم افزارهای واحد دارد و در صورت کمبود کارشناس در واحد فناوری اطلاعات هر مرکز واگذاری بخشهایی از کار(وظایف غیر حاکمیتی) به بخش خصوصی بلامانع است. تشخیص حجم کار و تعداد نیرو با استعلام و بررسی مدیریت آمار و فناوری اطلاعات دانشگاه خواهد بود.
- ۲- تامین تجهیزات سخت افزاری یا امکانات نرم افزاری (از قبیل تهیه نسخه پشتیبان از داده و ...) جهت تحقیق شرح وظایف ابلاغی، بر عهده مدیر محترم مرکز می باشد.

وظایف رئیس / مسئول واحد فناوری اطلاعات

۱. مدیریت، نظارت بر عملکرد و اجرای نرم افزارهای مرکز با همکاری شرکت پشتیبان
۲. نظارت، پایش و نگهداشت تجهیزات سخت افزاری کامپیوترهای، پرینترها اتاق سرور (سرورها، سویچ ها و...) و ...
۳. تعامل و برگزاری جلسات فنی با شرکت ها و موسسات همکار در اجرای فرایندهای مرکز
۴. اعلام نیازهای آموزشی به فناوری اطلاعات و ارتقا سطح علمی و عملی پرسنل زیرمجموعه
۵. مدیریت، نظارت و کنترل عملکرد پرسنل زیرمجموعه فناوری اطلاعات
۶. تحلیل و آنالیز فرآیند ها جهت مکانیزه شدن
۷. نظارت بر توسعه سامانه های جاری مرکز توسط شرکت های پشتیبان
۸. برنامه ریزی برای شرکت طرف قرارداد جهت راه اندازی و استقرار سامانه های جدید
۹. بررسی و تایید یا عدم تایید درخواست های تولید یا توسعه نرم افزار توسط واحدهای بهره بردار زیر مجموعه
۱۰. نظارت بر حفظ و نگهداری و امنیت سرورها، شبکه و توسعه سخت افزاری
۱۱. بررسی و تایید یا عدم تایید خرید تجهیزات سخت افزاری
۱۲. نظارت بر اجرای مفاد قراردادهای حوزه فناوری اطلاعات
۱۳. همکاری با وزارت متبوع درخصوص راه اندازی سامانه های کشوری
۱۴. شرکت در جلسات مرتبط با فرایندهای گسترش، اصلاح و ارتقا حوزه فناوری اطلاعات واحدهای زیرمجموعه مرکز
۱۵. پاسخگویی به مسئولین مافوق درامور مرتبط با حوزه فناوری اطلاعات بر اساس شرح وظایف
۱۶. نظارت و همکاری دوره های آموزشی و کارگاه های مربوط جهت یادگیری سامانه های جدید با همکاری شرکت مجری
۱۷. برنامه ریزی و نظارت بر فرایندهای مرتبط به امنیت تجهیزات سخت افزاری، زیرساخت، نرم افزار و سامانه های مرکز
۱۸. بررسی فنی علت نیاز به خرید تجهیزات رایانه ای و تایید یا عدم تایید نیاز یا تغییر در مشخصات فنی تجهیزات
۱۹. تایید فاکتورها از نظر فنی و مطابقت با لیست تجهیزات و بررسی قیمت و اعلام نظر احتمالی در زمینه قیمت ها (تایید قیمت مشمول قانونهای معاملاتی دانشگاه می شود)
۲۰. پیگیری اخذ تایید فنی مدیریت فن آوری اطلاعات دانشگاه بر خرید انجام گرفته در مورد اقلام خاص
۲۱. - شناسایی و تدوین شرایط درخصوص موارد قابل واگذاری حوزه فناوری اطلاعات واحد به بخش خصوصی

مسئول واحد فناوری اطلاعات :

دارای حداقل مدرک کارشناسی مرتبط یا حداقل ۵ سال سابقه کار مرتبط (برای افراد با رشته غیر مرتبط) در واحدهای فناوری اطلاعات دانشگاه باشد و بر اساس صلاحیت سنجی و طی مراحل اداری و موافقت مدیر مافوق و مدیریت فناوری اطلاعات و ارتباطات دانشگاه تعیین خواهد شد.

شرح وظایف کارشناسان IT :

(۱) وظایف عمومی کارشناسان فناوری اطلاعات:

ماده ۱ - تهیه و به روز نگاه داشتن، شناسنامه و مستندات تجهیزات رایانه ای، تجهیزات شبکه های کامپیوتری و زیرساخت های ارتباطی، شناسنامه نرم افزارها و یا پایگاههای داده موجود.

ماده ۲ - انجام مراحل کارشناسی فنی خرید و تایید یا عدم تایید فاکتورهای خرید در محدوده سقف مجاز در بخشنامه های ارسال شده از طرف مدیریت خدمات پشتیبانی دانشگاه (معاملات کوچک) و در معاملات بزرگ با هماهنگی اداره فن آوری اطلاعات و ارتباطات مطابق آیین نامه مالی و معاملاتی دانشگاه

ماده ۳ - حضور مستمر در جلسات هماهنگی و بازآموزی های برگزار شده توسط فن آوری اطلاعات و ارتباطات با نظر مسئول مافوق

ماده ۴ - پیگیری و رعایت بخش نامه ها یا دستورالعمل های ارسالی از طرف مراجع داخل دانشگاهی یا کشوری در حوزه فناوری اطلاعات

ماده ۵ - شناسایی شرایط درخصوص موارد قابل واگذاری به بخش خصوصی و اعلام به مدیریت مستقیم و مدیریت آمار و فناوری اطلاعات.

ماده ۶ - مستند سازی اقدامات تخصصی و زیربنایی اجرا شده در مرکز

ماده ۷ - ارائه راهکارها و گزارشات فعالیت های جاری انجام شده و اشکالات احتمالی فنی به همراه پیشنهادات مربوطه

ماده ۸ - مطالعه و تحقیق در زمینه روزرسانی و ارتقا فرایندهای جاری مرتبط در حوزه فناوری اطلاعات و آرایه راهکارهای مناسب به مقام

مافوق

ماده ۹ - تهیه دستورالعمل ها ، فایل های آموزشی ، برنامه های آموزشی جهت بهبود عملکرد بهتر پرسنل

ماده ۱۰ - پشتیبانی و نگهداشت سامانه های واسط عمومی (اتوماسیون اداری ، وب سایت مرکز و)

ماده ۱۱ - نظارت بر عملکرد کاربران حوزه فناوری اطلاعات و ارائه گزارش در خصوص کاربران ضعیف این حوزه به مدیریت مجموعه

۲) وظایف اختصاصی کارشناسان فناوری اطلاعات:

بطور کلی در چهار حوزه سخت افزار، شبکه، نرم افزار و امنیت می باشد:

۲-۱- وظایف در حوزه سخت افزار:

۱-۲-۱- نظارت بر روند خرید تجهیزات رایانه ای:

- تهیه لیست تجهیزات مناسب با نیاز(در صورت تایید نیاز) طبق مشخصات ارائه شده از سوی مدیریت فناوری اطلاعات و ارتباطات دانشگاه

۲-۲-۱- کنترل فنی تجهیزات خریداری شده از نظر تطبیق با فاکتور های تایید شده، به صورت زیر:

- بررسی فنی قطعات و گارانتی های ارائه شده و مطابقت با لیست تجهیزات خریداری شده (تجهیزات خریداری شده قبلاً باید توسط مسئول واحد فناوری یا مدیریت فناوری اطلاعات دانشگاه تایید شده باشد)
- تکمیل فرم مخصوص چک لیست سیستم همراه با توضیحات مربوطه
- موارد مربوط به خرید تجهیزات شبکه

۳-۲-۱- فرآیند تعمیرات:

- نصب یا به روز رسانی سیستم عامل ها و نرم افزارهای کاربردی (حسب تشخیص مسئول فناوری اطلاعات)، آنتی ویروس و... بر روی رایانه های موجود در واحد
- تشخیص عیوب سخت افزاری سیستم ها و رفع عیوب تجهیزات از طریق تعویض یا تعمیر تجهیزات توسط شرکتهای پشتیبانی یا فروشنده
- نظارت بر فرآیند ارسال تجهیزاتی که نیاز به تعمیر دارند (مانند: چاپگر) به شرکت های خصوصی، کنترل کیفیت تعمیر تجهیزات و تایید یا عدم تایید هزینه تعمیرات در موارد جزء (زیر سقف معاملات کوچک)
- تبصره - نظارت بر فعالیت شرکت های پیمانکار طرف قرارداد از طریق چک لیست های نظارتی و تایید یا عدم تایید صورت وضعیت های پیمانکار

۲-۲- وظایف در حوزه شبکه:

- ۱-۲-۲- نگهداری فنی از کلیه تجهیزات شبکه اعم از Active و Passive بر اساس استاندارد های فن آوری اطلاعات و ارتباطات
- ۲-۲-۲- تهیه مستندات فنی جامع شبکه بر اساس استانداردهای فناوری اطلاعات و ارتباطات
- ۳-۲-۲- آگاهی کامل از کاربرد و نحوه عملکرد تجهیزات Active
- ۴-۲-۲- آگاهی کامل از نوع ارتباط مرکز تا سایت دانشگاه و نحوه دسترسی به شبکه اینترنت و اینترنت و ارتباط با سایر شبکه های احتمالی موجود
- ۵-۲-۲- آگاهی کامل از نحوه عیب یابی درونی شبکه و رفع مشکلات احتمالی
- ۶-۲-۲- حفظ، نگهداری، پشتیبانی و عیب یابی از نقطه ابتدایی تا انتهایی شبکه موجود
- ۷-۲-۲- عیب یابی و رفع مشکلات ارتباطی کلیه سیستمهای کامپیوتری موجود در مرکز مربوطه (IP و کارت شبکه و...)
- ۸-۲-۲- مطلع بودن از انجام هرگونه عملیات عمرانی و تلاش جهت حفظ و نگهداری تجهیزات شبکه
- ۹-۲-۲- حفظ و نگهداری و عیب یابی روتر یا سوئیچ اصلی مرتبط با دانشگاه و بستر فیزیکی ارتباط اعم از فیبر نوری، وایرلس، اینترنت و تجهیزات مرتبط با آنها

۲-۲-۱۰- مطلع نمودن کارشناسان مدیریت آمار و فناوری اطلاعات دانشگاه جهت هرگونه توسعه تجهیزات شبکه داخلی اعم از کم و زیاد نمودن اکسس پوینت های داخلی و بین مراکز و همچنین هرگونه تغییر در ساختار و تنظیمات تجهیزات موجود

۲-۳- حوزه نرم افزار :

۳-۲-۱- نرم افزار و پایگاه داده

- نگهداری و حفاظت فنی و سایبری از منابع اطلاعاتی و سامانه های تحت پوشش مرکز بر اساس ضوابط ابلاغی پیگیری و ارائه راهکارهای مناسب جهت رفع مشکلات نرم افزاری و بهبود سیستم
- مشاوره فنی به واحدهای متقاضی جهت الکترونیکی کردن فرایند های کاری آن واحد و نظارت بر تهیه RFP سامانه های نرم افزاری
- هماهنگی با مدیریت فناوری اطلاعات در خصوص عقد قراردادهای تولید، توسعه یا پشتیبانی نرم افزارها
- آشنایی فنی با نرم افزار ها و سخت افزارهای تحت پوشش واحد فناوری اطلاعات
- آگاهی از کلیات (حیطه و نوع فعالیت های تحت پوشش) نرم افزارهای واحد مربوطه جهت پیگیری مناسب تر مسائل مربوطه
- تهیه فایل پشتیبان (Backup data) از پایگاه داده یا فایل های اطلاعاتی نرم افزار ها بصورت دوره ای و آرشیو آنها و صحت سنجی نسخ پشتیبان
- تایید اتمام کار پروژه ها و صورت وضعیت ها یا فاکتور های نرم افزاری
- نظارت بر هر گونه تغییر و تحول نرم افزار های زیر مجموعه

۳-۲-۲- پشتیبانی و نظارت فنی بر سامانه ها

کلیه امور کاربری و محتوایی سامانه ها به سوپروایزر برنامه (فردی غیر از کارشناس یا مسئول فناوری اطلاعات) و شرکت پشتیبان مربوط می باشد و تنها نظارت فنی و رفع اشکال جهت اتصال و ورود بر سامانه ها بر عهده مسئول یا کارشناس **IT** مرکز می باشد .

*وظائف مسئولین **IT** در خصوص سامانه سمکا (توزیع اینترنت کاربران غیر هیئت علمی با دانشجو) :

- ۱- بررسی و تایید شرایط متقاضیان اکانت vpn
- ۲- درخواست اکانت vpn با تایید بالاترین مقام مسئول واحد بصورت کتبی و یا از طریق اتوماسیون اداری
- ۳- رعایت ضوابط تخصیص اعتبار کاربر در ساعات اداری و غیر اداری
- ۴- ثبت مشخصات متقاضی در سامانه سمکا
- ۵- تحویل کد کاربری و رمز عبور به فرد متقاضی
- ۶- پشتیبانی کاربران در هنگام بروز مشکل
- ۷- غیر فعال و حذف کردن اکانت کاربرانی که دیگر واجد شرایط دریافت اکانت نمی باشند.

۳-۲-۳- محتوای وب سایتها :

شرح وظائف مربوط به محتوای وب سایتها به شرح ذیل می باشد که توسط مسئول IT باید به مسئول روابط عمومی مرکز ارجاع گردد.

- تهیه و تنظیم مطالب و افزودن مطالب به وب سایت
- ایجاد منوهای مورد نیاز
- فعال سازی منو های در بلوک ها
- ایجاد بلوک هادر و ب سایت
- ساخت فرم های مورد نیاز واحد
- تنظیم پست الکترونیک در وب سایت
- ایجاد مجموعه ها و فهرست های مورد نیاز مطالب
- بروز رسانی مطالب وب سایت
- نکته: مسئولیت هر گونه خبر، تصویر یا محتوایی که بر روی وب سایت قرار می گیرد و یا لینک به وب سایت های خارجی (بیرونی) بر عهده مسئول محتوای وب سایت می باشد.

۳-۲-۴- اتوماسیون اداری :

- انجام مکاتبات مربوط به تغییرات در دیدگاه (لازم است پیشنهاد مکاتبات توسط راهبر تهیه شده و با امضای افراد صاحب امضا و مجاز، به مدیریت فاوا اعلام گردد)
- انجام تنظیمات مورد نیاز نرم افزار در سطح ویندوز یا browser
- آموزش اتوماسیون اداری به کاربران جدید در هر سطحی در آن مرکز
- پاسخگویی به اشکالات و سوالات کاربران
- بررسی و تشخیص رخداد خطاها و انتقال صحیح آن به کارشناسان اتوماسیون اداری
- انتقال مشکلات نرم افزار به کارشناسان اتوماسیون اداری از طریق تیکت یا تلفن یا هر روش دیگری که اعلام خواهد شد
- بررسی صحت ورود اطلاعات و صحت استفاده از نرم افزار توسط کاربران مطابق دستورالعمل های ارسالی از جانب مدیریت فناوری اطلاعات
- نصب هر نوع نرم افزار مورد نیاز سامانه چارگون که از طریق کارشناسان اتوماسیون اداری اعلام میگردد
- شرکت در کلاسهای آموزشی اعلام شده توسط کارشناسان اتوماسیون اداری

۳-۲-۵- وظایف در حوزه پورتال :

- انجام مصاحبه جهت شناسایی فرآیندها، تهیه سند توصیف نیازمندی ها، ارزیابی امکان پیاده سازی نیاز اعلام شده
- واحد و ارجاع نیازهای مصوب شده واحد به کمیته پورتال
- تحلیل و طراحی فرم ها و فرآیندهای ارجاعی از کمیته پورتال در زیر پورتال حوزه خود

- ایجاد گزارشات و کارتابل جهت فرآیندهای ارجاعی از کمیته پورتال در زیر پورتال حوزه خود
- انعکاس مشکلات موجود در سامانه پورتال از طریق تیکت یا تلفن یا هر روش دیگری به راهبران سامانه (مشکلات کاربری و مشکلات طراحی و گردش کار)
- ارائه پیشنهادات و رویکردها و روشهای نوین کاری برای انجام کارآمد وظایف و بهبود عملکرد رابطین و کاربران سامانه به راهبران سامانه
- شرکت در دوره های آموزشی تخصصی رابطین سامانه پورتال اعلام شده توسط مدیریت آمار و فناوری اطلاعات.
- آموزش فرآیندهای طراحی شده به ذینفعان فرآیند در هر سطحی در آن مرکز.
- پاسخگویی به اشکالات و سوالات کاربران در حوزه خود
- ارسال درخواستهای تغییرات نقش ها در حوزه مربوطه (تغییر یا ایجاد نقش امنیتی ، تغییر یا ایجاد نقش کاربری و ...) به راهبران سامانه
- به روز رسانی فهرست فرآیندهای طراحی شده در وب سایت مرکز مربوطه (در صورت نیاز)

۳-۲-۶- وظائف مسئولین PACS_ HIS و ...

- ایجاد هماهنگی جهت ارائه آموزش های لازم از طرف شرکت پیمانکار به کاربران براساس نیازمندی های آموزشی کاربران.
- طرح درخواست های بهبود و توسعه مربوط به برنامه در کمیته های بیمارستان .
- طرح مصوبات در کمیته فنی مشترک شرکت پشتیبان و واحد مدیریت فناوری.
- ارسال صورت وضعیت ماهیانه عملکرد پشتیبانی شرکت پیمانکار بر اساس سامانه تیکتینگ تا پانزدهم ماه بعد.
- انتقال مشکلات احتمالی از طرف شرکت پیمانکار یا کاربری نرم افزار به کارشناسان مدیریت آمار و فناوری اطلاعات
- تهیه پشتیبان از داده های سامانه ها در بازه های زمانی مناسب و خارج از سرور اصلی
- نظارت بر ثبت دقیق و واضح مشکلات ، بهبود ها و توسعه های درخواستی بیمارستان در سامانه تیکتینگ .
- هماهنگی جهت ایجاد دسترسی به مسئولین واحدها جهت ثبت تیکت های درخواستی خود و بررسی و ارسال به موقع تیکت ها برای شرکت پیمانکار.
- پیگیری جهت حل به موقع موارد ذکر شده در تیکت ها توسط شرکت پشتیبان.
- بررسی تیکت های بسته شده توسط شرکت پشتیبان و بستن تیکت در صورت تایید یا باز کردن تیکت در صورت عدم تایید رفع مشکل درج شده در تیکت.

۴-۲- حوزه امنیت :

- اجرای کلیه الزامات و ضوابط ابلاغی مراجع ذیصلاح در سطح ملی، استانی و دانشگاهی
- بررسی و حصول اطمینان از ایمنی ساختار شبکه، اطلاعات، داده ها و سیستم های نرم افزاری و سخت افزاری مجموعه
- پیش بینی و اعمال راهکارهای لازم جهت حفظ امنیت شبکه در سطوح و لایه های مختلف
- به روزرسانی دانش فنی در زمینه امنیت و امکان سنجی برای پیاده سازی
- اجرای راهکارها و استانداردهای رعایت اصول امنیت داده ها

- استقرار، پیکربندی و پشتیبانی از ابزار ها و محصولات امنیتی نظیر فایروال ها، نرم افزار های آنتی ویروس ، سیستم های مدیریت Patch (وصله) های امنیتی ، و غیره
- پیاده سازی سیاست های امنیتی در حوزه های مختلف شبکه و زیرساخت ارتباطی، نرم افزار، کنترل دسترسی، حفاظت از اطلاعات سازمان و...
- برنامه ریزی و اجرای آزمون و تست نفوذ بروی منابع مختلف (سرورها، نقاط پایانی، برنامه های کاربردی وب، شبکه های بی سیم یا وایرلس، دستگاه های داخل شبکه، دستگاه های موبایل، سایر نقاط بالقوه)
- اجرای راهکارهای مناسب بمنظور جلوگیری از نفوذ و نشت اطلاعات
- پشتیبان گیری منظم از تمامی سرویس ها، سامانه های حیاتی، داده های عملیاتی، آخرین نسخه پیکر بندی تجهیزات و سامانه ها
- پیکربندی تجهیزات، نرم افزارهای مرتبط با سامانه های حیاتی بر اساس آخرین راهنمایی های امنیتی مربوطه
- مدیریت کنترل دسترسی شامل هر نوع دسترسی به داراییهای سازمانی اعم از فیزیکی یا منطقی، راه دور یا محلی
- طراحی و اجرای ساختار شبکه براساس استانداردهای امنیتی