دانشگاه علوم پزشکی و خدمات
بهداشتی درمانی استان زنجان

دستورالعمـــل
نگهداری سیستم های رایانه ای

تهیه و تنظیم:

واحد فناوری اطلاعات و ارتباطات

مرکز بهداشت شهرستان زنجان

مقدمه

با توجه به گسترش روز افزون استفاده از تکنولوژی فناوری اطلاعات و ارتباطات در ارائه خدمات به شهروندان و وابستگی عملیات جاری مراکز بهداشت و عملکرد صحیح و بدون وقفه تجهیزات رایانه‌ای، نگهداری و استفاده صحیح از امکانات موجود اهمیت ویژه ای یافته است. در این راستا شیوه نامه حاضر با هدف ارائه استاندارد استفاده از تجهیزات عمومی در اختیار همکاران تشریح شده است تا با رعایت دقیق مفاد آن شاهد کاهش آسیب به تجهیزات و بروز وقفه در عملیات جاری اداری باشیم.

کلیات و مقررات عمومی

۱- کاربر چنانچه از قبل رایانه نداشته باشد جهت استفاده از رایانه باید ابتدا درخواست تجهیزات رایانه‌ای خود را از طریق مقام ارشد اداره به واحد فناوری اطلاعات و ارتباطات ارسال نموده و تجهیزات رایانه ای را طبق مقررات مرکز بهداشت شهرستان زنجان و با امضاء صورتجلسه مربوطه تحویل بگیرد.

۲- کلیه تجهیزات رایانه‌ای باید دارای کد اموال مرکز بهداشت و یا سازمان‌های تابعه بوده و کاربر موظف است در ابتدای تحویل وجود کد اموال روی تجهیزات رایانه‌ای را چک نموده و سپس تحویل بگیرد و در صورت نداشتن کد اموال روی تجهیزات رایانه‌ای باید به جمع دار اموال محل خدمت خود مراجعه و درخواست کد اموال نمود و نصب نمایید.

۳- کلیه تجهیزات رایانه مستقر در مراکز بهداشت می‌بایست برچسب پلمپ سازمان فناوری اطلاعات را داشته و مسئولیت حفظ و نگهداری از آن و جلوگیری از باز شدن آن به عهده کاربر مربوطه می باشد.

۴- در صورت بروز هرگونه مشکل در تجهیزات رایانه‌ای سخت افزاری و نرم افزاری شبکه و غیره کاربر باید ابتدا مراتب را به اطلاع کارشناس واحد انفورماتیک و در صورت عدم حضور به اطلاع امور اداری محل خدمت خود برساند بدیهی است کاربر راساً حق اقدام بدون اطلاع مسئولین ذکر شده را ندارد.

۵- در صورت تشخیص کارشناس مسئول رایانه هر واحد مبنی بر نیاز ارسال تجهیزات رایانه‌ای به واحد انفورماتیک مرکز بهداشت برای انجام تعمیرات و یا نصب نرم افزار خاص لازم است فرم مخصوص خدمات پشتیبانی و نگهداری را که الزامی بوده به صورت کتبی تکمیل و پس از تکمیل و تایید مسئولین ذیربط و همراه تجهیزات به سازمان ارسال نماید.

دستورالعمل ها

۱- کاربر مجاز است از رایانه خود فقط جهت نرم‌افزارهایی که از طرف مسئولین مربوطه برای آن تعریف شده است استفاده نمایند و هرگونه تلاش برای نصب نرم‌افزارهای خارج از حیطه تعیین شده (اعم از انواع نرم افزارهای کاربردی غیر مرتبط، غیرمجاز، گرافیکی، افزودنی های تزئینی، بازی ها و ...) به هر شکل خودداری نمایند. در صورت مشاهده این گونه موارد کاربرد رایانه مسئول شناخته می‌شود.

۲- اطلاعات رایانه مراکز بهداشتی (اعم از تصاویر، جداول، پرونده‌ها، اسناد، پرونده های رایانه ای و ...) داخل شبکه و سرور ها و یا بر روی رایانه ها، متعلق به مرکز بهداشت بوده و برای انجام امور جاری اداری است. هرگونه خارج نمودن و انتشار آنها نیاز به اخذ مجوز از مقامات ذیصلاح مربوطه دارد.

۳- هرگونه اقدامی که منجر به اختلال در عملکرد تجهیزات رایانه‌ای شبکه و دیگر کاربران گردد اکیداً ممنوع بوده و کاربر متخلف مسئولیت عواقب مربوطه را دارد

۴- هرگونه اقدامی که منجر به تخریب اطلاعات رایانه در اختیار کاربر یا دیگر کاربران گردد (مستقیم یا غیر مستقیم) اکیداً ممنوع است.

۵- ایجاد و توسعه شبکه یا تغییر در تنظیمات شبکه، IP سیستم ها و اضافه کردن IP منحصراً توسط کارشناسان واحد فناوری اطلاعات و ارتباطات صورت می‌پذیرد به اقدام توسط کاربران و کارشناسان رایانه‌ای بدون مجوز، اکیداً ممنوع بوده و ارتکاب آن تخلف امنیتی محسوب گشته و مرتکبین به حراست معرفی می گردند.

۶- هرگونه تلاش نرم افزاری و سخت افزاری جهت نفوذ به سایر کلاینت ها، سرور ها و دیتابیس ها، که جزء دسترسی مجاز یک کاربر نمی باشد اکیداً ممنوع است .

۷- کاربر موظف است از رایانه خود و لوازم جانبی مربوطه مواظبت لازم را به عمل آورده و همواره پلمپ بودن کیس خود را زیر نظر داشته باشد زیرا ارائه خدمات از طرف واحد فناوری اطلاعات و ارتباطات مرکز بهداشت منوط به صحت برچسب پلمپ بوده و مسئولیت حفظ آن به عهده کاربر تحویل گیرنده می باشد.

۸- باز کردن و تلاش در تعمیر کردن کیس ها تجهیزات شبکه و تجهیزات جانبی رایانه از جمله پرینتر، اسکنر و غیره توسط کاربران اکیداً ممنوع می‌باشد. انجام تعمیرات صرفاً توسط کارشناسان و پیمانکاران واحد فناوری اطلاعات و ارتباطات صورت می پذیرد.

۹- ورود بدون اخذ مجوز لازم به سیستم نرم‌افزار شبکه یا نام کاربری و کلمه عبور دیگران به هر عنوان ممنوع می باشد و مصداق سوء استفاده و سعی در دستیابی به اطلاعات به صورت غیرمجاز بوده و قابل پیگیری می باشد.

۱۰- نگهداری و نصب و راه اندازی و استفاده از هرگونه نرم افزار هک، اسنیفر، کرک، کی لاگر، مانیتورینگ، ریموت کنترل، فیلتر شکن و غیره (حتی به صورت برنامه نصب نشده) که امنیت شبکه مراکز بهداشت را مخدوش نموده و باعث ایجاد درگاه برای ورود غیرمجاز به سیستم و شبکه می‌شود اکیداً ممنوع می باشد.

۱۱- کاربران موظفند اطلاعات مورد نیاز خود را صرفاً در فضای رایانه خود نگهداری نمایند و از کپی نمودن آن در هر مکان دیگری خودداری نمایند در غیر اینصورت مسئولیت ازبین‌رفتن و مخفی شدن آن صرفاً به عهده کاربر می باشد.

۱۲- هرگونه کپی اطلاعات شخصی، خانوادگی و غیرسازمانی بر روی رایانه یا بر روی منابع به اشتراک گذاشته شده در شبکه (Share) یا FTP ممنوع است.

۱۳- کاربران، مجاز به مراجعه و بازدید سایت های اینترنتی که بر اساس قوانین جمهوری اسلامی ایران غیر مجاز شناخته شده اند نمی باشند.

۱۴- استفاده از اینترنت در محیط کاری صرفاً جهت استفاده در موارد مرتبط با وظیفه اداری کاربران مجاز است. لذا استفاده از اینترنت جهت دریافت هرگونه اطلاعات غیر مرتبط با وظیفه اداری، استفاده از انواع مسنجر، همچنین سایتها و وبلاگهایی که به لحاظ محتوا سنخیتی با فعالیت‌های اداری کاربر ندارند ممنوع میباشد.

۱۵- دسترسی به اینترنت برای هر کاربر فقط در محدوده زمانی مشخص که از طریق مسئولان مربوطه می‌گردد مجاز است هر گونه تلاش برای دستیابی به اینترنت خارج از حیطه تعیین شده اکیداً ممنوع می باشد.

۱۶- به دلیل محدودیت پهنای باند بارگذاری (download) نرم افزار اطلاعات و داده ها توسط کاربر ممنوع بوده و کارشناسانی که حسب وظیفه ویژه خود اجازه بارگزاری محدود اطلاعات را دارند، باید در ساعات خلوت اداری و بدون استفاده از نرم افزارهای مدیریت بارگذاری (Download Manager) اقدام به بارگذاری نمایند.

۱۷- به طور کلی هرگونه استفاده از فیلتر شکن مانند VPN، HTTPS، SOCKS ممنوع است.

۱۸- در هنگامی که به سیستم خود نیازی ندارید یا به هر دلیلی آن را ترک می نمایید برای زمان‌های کوتاه (در حد چند دقیقه) آنرا lock و برای زمانهای بلندتر آن را Logoff نمایید. بدیهی است که مسئولیت هرگونه سوء استفاده از رایانه کاربر، توسط افراد غیر مجاز در زمان غیبت کار بر عهده کاربر سیستم می باشد همچنین باید در پایان ساعت اداری حتماً سیستم خود را خاموش نموده و میز خود را ترک نمایید.

۱۹- استفاده از CD و DVD رایتر، DVD رایتر اکسترنال و فلش جهت انتقال فایل به رایانه ها به طور کلی ممنوع است. کلیه نقل و انتقال فایل ها باید با کسب مجوزهای لازم انجام پذیرد در صورت نیاز به ورود اطلاعات به رایانه فقط توسط CD و DVD امکان‌پذیر خواهد بود. کاربران مجاز جهت کپی اطلاعات بر روی CD و DVD باید از رایانه‌های در نظر گرفته شده برای انجام این کار که با تشخیص کارشناسان واحد انفورماتیک تعیین گردیده اقدام لازم را انجام دهند.

۲۰- از فضای به اشتراک گذاشته شده در شبکه (Share) برای نگهداری اطلاعات نباید استفاده نمود. بنابراین نگهداری از اطلاعاتی که نیاز به تهیه پشتیبان دارند باید با هماهنگی کارشناسان واحد انفورماتیک صورت پذیرد.

۲۱- اتصال موبایل، تبلت، دوربین دیجیتال توسط کابل، بلوتوث و غیره به رایانه، توسط کاربران حتی جهت شارژ دستگاه ممنوع است. تنها اتصال دوربین های متعلق به مرکز بهداشت در واحدهای مجاز (سمعی و بصری ،روابط عمومی و بهداشت محیط) جهت انتقال اطلاعات بر روی رایانه با کسب مجوز از کارشناسان سازمان فناوری اطلاعات و ارتباطات امکان پذیر می باشد.

۲۲- پسورد BIOS مادربرد، پسورد Local Admin و دیگر پسورد های مدیریتی شبکه انحصاراً باید در اختیار کارشناسان واحد فناوری اطلاعات و ارتباطات بوده و به هیچ عنوان کاربران و دیگر کارشناسان غیرمجاز حق دستیابی و استفاده از آن را ندارند.

۲۳- برنامه های مانند آنتی ویروس ها، سرویس های نصب شده و ... بر روی کلاینت ها نباید تغییر وضعیت داده شده (متوقف- Stop) یا غیرفعال گردند.

۲۴- هرگونه تغییر در پالیسی فایروال دسترسی و ریست کردن پسورد بر روی دستگاه های کاربر ممنوع بوده و در موارد خاص و فقط توسط کارشناسان سازمان فناوری اطلاعات و ارتباطات انجام می پذیرد.

۲۵- تهیه هرگونه نسخه پشتیبان و (Backup) از اطلاعات سرور ها شامل دیتابیس ها، فایلها و دایرکتوری ها، منحصراً توسط کارشناسان واحد فناوری اطلاعات و ارتباطات دارای مجوز مجاز است و اقدام توسط کاربران و کارشناسان دیگر در رابطه با دستیابی و تهیه نسخه پشتیبان از اطلاعات سرورها و سیستم های رایانه ای را به منزله تلاش در دستیابی به اطلاعات به صورت غیرمجاز بوده و قابل پیگیری می باشد.

تبصره مهم: در صورتی که کاربران اطلاعات حائز اهمیتی روی رایانه خود داشته باشند (نظیر نامه‌های مهم، متن قراردادها، آمارها، عکس ها و ...) خود مسئول تهیه نسخه پشتیبان می باشد و این کار را باید با هماهنگی کارشناسان واحد انفورماتیک انجام رسانند.

۲۶- کاربران موظفند حداقل هفته ای یکبار از به روز بودن آنتی ویروس خود اطمینان حاصل نموده و در ساعاتی که استفاده زیادی از رایانه خود ندارند، سیستم خود را با آنتی ویروس اسکن کامل نمایند و در صورت بروز نبودن آنتی ویروس، سریعاً به کارشناسان واحد انفورماتیک اطلاع دهند. در صورت نیاز به هرگونه جابجایی و تغییر و تحول در محل، لازم است قبل از اقدام به جابجایی و پس از مشخص شدن محل جدید با ارسال درخواست به واحد فناوری اطلاعات و ارتباطات جهت بررسی محل جدید از نظر تجهیزات و نودهای شبکه و دیگر زیرساخت ها اقدام لازم به عمل آید.

راهنمای استفاده از پرینتر

۱- در صورت گیر کردن کاغذ داخل پرینتر به هیچ عنوان با زور، کاغذ را بیرون نکشید زیرا باعث شکسته شدن محور پیکاپ و صدمه دیدن دستگاه می گردد. در این گونه موارد برای خارج کردن کاغذ ابتدا کارتریج دستگاه را خارج کرده و سپس در پشت پرینت را باز نموده آنگاه در صورت امکان از پشت دستگاه به آرامی کاغذ را خارج کنید و در صورت امکان پذیر نبودن این امر از جلوی دستگاه به آرامی اقدام به خارج کردن کاغذ نمایید.

۲- چنانچه بعد از گرفتن تعدادی پرینت و گرم شدن دستگاه به صورت مداوم کاغذ در آن را دستگاه گیر می‌کند. جهت رفع مشکل به مسئول رایانه یا کارشناس واحد انفورماتیک در محل اطلاع دهید.

۳- در صورت پاره شدن کاغذ در دستگاه خارج شدن کاغذ ناقص کاغذی که قسمتی از آن داخل دستگاه گیر کرده است شبیه به بند یک عمل کرده و کاغذ را خارج نمایید و در صورت پیدا نکردن تکه گمشده کاغذ داخل دستگاه با آن دستگاه پرینت نگیرید زیرا باعث صدمه دیدن پرینتر می گردد جهت رفع مشکل به مسئول واحد یا کارشناس واحد انفورماتیک اطلاع دهید.

۴- کاغذ دارای منگنه سوزن ته گرد و یا هر شیء دیگر را در پرینتر قرار ندهید زیرا باعث پاره شدن فیلم فیوزینگ یا شکستن چرخ دنده های پرینتر می گردد.

۵- کاربر موظف است اهرم های تنظیم سایز کاغذ را درسینی کاغذ کش متعاقبا سایز کاغذ روی فِلش های مشخص شده تنظیم نماید و در صورت عدم تنظیم سایز کاغذ توسط اهرم ها باعث شکسته شدن محور پیکاپ و گیر کردن کاغذ در دستگاه می‌شوند.

۶- پر کردن بیش از حد کاغذ درون سینی کاغذ کش باعث گیر کردن کاغذ در دستگاه می گردد.

۷- هرگونه تغییر در تنظیمات پرینتر ها و تنظیمات شبکه پرینتر های دارای کارت شبکه توسط کاربران ممنوع می باشد و این تغییرات باید توسط مسئول رایانه کارشناس واحد انفورماتیک صورت پذیرد.

۸- کاربرانی که از پرینترهای رنگی جوهر افشان استفاده می کنند جهت خشک نشدن جوهر کارتریج دستگاه باید حداقل یکبار در هفته اقدام به گرفتن پرینت رنگی یا تست پرینتر نمایند.

۹- کاربر باید نهایت دقت را در نگهداری از دستگاه پرینتر خود به خصوص درب جلویی دستگاه را بنماید چون در صورت شکسته شدن قطعات آن قابل تعمیر نمی باشد و همچنین مراقبت لازم جهت جلوگیری از ریختن هرگونه مایع و شی خارجی به داخل پرینتر و عمل آورد زیرا باعث صدمه دیده دستگاه یا شکستن چرخ دنده های دستگاه می شود.

۱۰- معمولاً پرینترهای رنگی دارای Cleaner می باشند که در صورت لزوم و جهت پاک کردن جوهر اضافی و خشک شده میتوان از آن استفاده کرد.

۱۱- گرفتن پرینت شخصی توسط پرینترهای مرکز بهداشت ممنوع می باشد و ارتکاب آن تخلف محسوب می گردد .

۱۲- کارتریج پرینترهای لیزری حداقل تا ۴ بار باید شارژ کرده و مجددا استفاده کرد و در صورت عدم امکان شارژ کارتریج توسط واحد استقرار پرینتر باید کارتریج های خالی را به واحد فناوری اطلاعات و ارتباطات، جهت شارژ ارسال نمایید. جهت تحویل گرفتن کارتریج های شارژ شده از واحد فناوری اطلاعات و ارتباطات نیاز به پر کردن فرم و تکمیل امضا های مربوطه می باشد.

۱۳- کاربر موظف است بعد از پایان ساعت اداری پرینتر را توسط دکمه پاور که در جلو یا پشت دستگاه تعبیه شده است خاموش نماید زیرا این دستگاه در حالت آماده به کار و مصرف انرژی بالایی دارد.

راهنمای استفاده از اسکنر

۱- جهت استفاده از قسمت تخت اسکنر با رعایت کامل ایمنی لولا در موقع باز و بسته کردن درب اسکنر که توسط لوله های پلاستیکی بهترین اتصال دارد اقدام نمایید .

۲- با توجه به اینکه سینی کاغذ کش اسکنرها از جنس پلاستیکی بوده و بسیار حساس می‌باشد لذا باید مواظبت کامل در حفظ و نگهداری آن به عمل آورده کاغذها را مناسب با ظرفیت دستگاه در آن قرار دهید.

۳- در موقع اسکن مدارک کاربر بایستی توجه نمایید که اسناد فاقد هرگونه منگنه، سنجاق، چسب، لاک غلط گیر، تاخوردگی و پارگی باشد تا صدمه به دستگاه وارد نگردد.

۴- در صورتی که نیاز به جدا کردن پورت USB اسکنر سیستم رایانه برای جابجایی دستگاه و غیره باشد باید جهت نصب مجدد اسکنر، سیستم رایانه از همان پورت USB که قبل از دستگاه به آن متصل بوده استفاده گردد در غیر این صورت نیاز به نصب مجدد نرم افزاری دستگاه و انجام تنظیمات آن و در بعضی از موارد نیاز به تعویض سیستم عامل می باشد

۵- با توجه به اینکه اسکنرهای حرفه ای دارای تنظیمات مخصوص نرم‌افزاری هستند اکیداً از هرگونه تغییر در نرم افزار اسکنر خودداری نمایید.

۶- کاربر موظف است بعد از ساعات اداری و در پایان کار دستگاه اسکنر خود را با سوئیچ پاور تعبیه شده در پشت دستگاه خاموش نماید.

راهنمای استفاده از مانیتور

۱- به هیچ عنوان مانیتورهای LCD را با شیشه پاک کن و مواد شوینده تمیز نمایید زیرا باعث تخریب و مات شدن صفحه نمایش دستگاه می گردد.

۲- رعایت گردد تا اشیای نوک تیز به صفحه مانیتور برخورد نداشته باشند.

۳- تنظیمات مانیتور تغییر داده نشود.

۴- کلیه برچسب های پلاستیکی مانیتور و پس از تحویل گرفتن مانیتور از روی آن بکنید زیرا مانع تبادل حرارتی دستگاه و صدمه دیدن دستگاه می‌گردد.

۵- در مواقع غیر لزوم و بعد از پایان وقت اداری مانیتور را خاموش نمایید.

تعاریف و واژگان

تجهیزات رایانه‌ای: به رایانه و کلیه متعلقات آن اعم از کیس، مانیتور، کیبرد، موس، پرینتر، اسکنر اسپیکر، بارکدخوان، لپتاپ، سوئیچ، کابل های شبکه و ... اطلاق می گردد.

کاربر: شخصی است که به صورت مجاز و با دارا بودن شناسه تعریف شده در شبکه (شامل نام کاربری و کلمه عبور) از سیستم های متصل به مراکز بهداشت و یا رایانه های مستقل آن استفاده می نماید. شمول این کلمه در تمام سطوح سازمانی از اپراتورها تا مدیران ارشد بوده و همچنین دربرگیرنده پرسنل مرکز بهداشت و یا افرادی است که به واسطه ارتباط تعریف‌شده با مرکز بهداشت مجاز به استفاده از سیستم‌های رایانه‌ای مرکز بهداشت می باشد

اطلاعات، داده ها: هرگونه اطلاعات خام یا پردازش شده که به نوعی مرتبط با مرکز بهداشتی واحدها و مجموعه های تابعه و مراکز بهداشت باشند و به صورت دیجیتالی در سیستم ذخیره شده باشند را شامل می شود. این اطلاعات می تواند به صورت متن و نوشته فیلم و عکس، فایل های صوتی، نقشه ها و اطلاعات جغرافیایی، تصاویر اسکن شده، اعداد و ارقام و ... باشد.

شبکه مرکز بهداشت: شبکه اصلی و گسترده (WAN) مرکز بهداشت از اتصال شبکه های کوچک تر از (LAN)سازمان‌های مرکز بهداشت حاصل می‌شود شامل تمامی ساختمان ها و مراکز بهداشت (مرکز، پایگاه‌ها، معاونت‌ها و سازمان‌ها) می‌باشد.

بکاپ، Backup نسخه پشتیبان: پشتیبانی و ذخیره سازی اطلاعات دیتابیس ها در محل های دیگر جهت، بازیابی اطلاعات هنگام وقوع اتفاقات پیش بینی نشده را گویند.

هک Hack: نفوذ کردن و دستیابی به اطلاعات دیتابیس ها، کامپیوترها، سرور ها و ... به صورت غیر مجاز میباشد که معمولاً توسط بدافزارهایی مانند اسنیفر ها، اسپای وارها، تروجانها، کی لاگرها، کراکرها، نرم افزار های ریموت کنترل و امثال آن انجام می شود .