سازمان فناوری اطلاعات و ارتباطات
شهرداری مشهد

پیش‌نویس آئین‌نامه نظام 5S مرتبط با حوزه فناوری اطلاعات

پائیز ۱۳۹۴

مقدمه:

نظام آراستگی منجر به پیشگیری از حوادث و افزایش بهره‌وری می‌گردد. شاید بهتر باشد بگوییم هدف نهایی 5S پیشگیری از اتلاف است. این نظام نخستین بار توسط ژاپنی‌ها به اجرا درآمد. قبل شروع بحث بهتر است به این نکته اشاره شود که 5S پیش‌شرط اجرای موفقیت‌آمیز سایر سیستم‌ها و مدل‌ها می‌باشد و مزیت آن این است که در همه‌جا قابل پیاده‌سازی است. اجرای 5S برای رسیدن به هدف‌های متعددی اجرامی‌شود. برخی از مهم‌ترین هدف‌ها عبارت‌اند از: ایمنی و بهداشت، بهره‌وری، صرفه‌جویی در هزینه‌ها، کیفیت و پیشگیری از خرابی‌ها در محیط‌هایی که با اجرای نظام آراستگی مدیریت می‌شوند، اشیا زائد و غیرضروری وجود ندارد و اقلام موجود بانظمی خاص مرتب می‌شوند و این امر تا حد زیادی موجب صرفه‌جویی و ایمنی محیط خواهد شد. اجرای منظم مراحل نظام آراستگی محیطی پاکیزه و بهداشتی را فراهم می‌آورد و از همه مهم‌تر تلاش برای ایجاد عادت‌های صحیح در کارکنان مهم‌ترین عامل در تحقق محیط‌های آراسته است و این مهم در اجرای بند پنجم حاصل خواهد شد. وجود محیطی سامان‌یافته از الزامات تولید یا ارائه خدمات باکیفیت است.

1. **هدف و دامنه کاربرد**

ارائه آئین‌نامه‌ای به‌منظور تشریح عوامل تشکیلاتی نظام آراستگی بر اساس اصول 5S با نگاه فناوری اطلاعات و ارتباطات و نیز رعایت الزامات ISMS

2. **مسئولیت**

مسئولیت حسن اجرای این آئین‌نامه از بعد فنی صرفاً بر عهده سازمان فناوری اطلاعات و ارتباطات می‌باشد. بدیهی است سایر مسئولیت‌ها که نگاه فنی نداشته باشد در حیطه این آئین‌نامه قرار نمی‌گیرد.

3. **شرح آئین‌نامه**

a. **طبقه‌بندی اطلاعات**

اطلاعات برای نشـان دادن نیاز، اولویت‌ها و میزان محافظت مورد انتظار با توجه به ارزش، الزامات قانونی، حســاســیت و بحرانی بودن برای ســازمان بایســتی طبقه‌بندی گردند. (اطلاعاتی که دارای درجه‌های حساسیت و بحرانی بیشتری هستند بایستی از محافظت بیشتری بهره‌مند گردند.)

- کلیه دارایی‌های اطلاعاتی سازمان با توجه به دسته‌بندی زیر شناسایی می‌گردند.
  - دارایی‌های فیزیکی
  - نرم‌افزارها
  - سرویس‌ها
  - منابع انسانی
  - مدارک و مستندات و اطلاعات
- می‌بایست سند رهنمود طبقه‌بندی در سازمان تهیه و تدوین گردد و در اختیار مسئولین مربوطه (مدیران واحدها) قرار گیرد.
- می‌بایست رهنمود طبقه‌بندی، مفادی برای طبقه‌بندی مقدماتی و طبقه‌بندی مجدد باگذشت زمان، مطابق با خط‌مشی کنترل دسترسی از پیش تعیین شده را شامل باشند.
- اطلاعات در محدوده ISMS به‌صورت ذیل طبقه‌بندی می‌گردد:
  - **محرمانه (Confidential)**

اطلاعات محرمانه، آن د سته از اطلاعات ک سب‌وکار می‌با شند که ب سیار ح ساس بوده و در اختیار افراد مجاز خا صی در داخل و خارج سازمان می‌با شد که حقوق د ستر سی آنان م شخص و م ستند گردیده. افشــای غیرمجاز این نوع اطلاعات می‌تواند اثر مخربی روی کســب‌وکار، مشــتریان، کارکنان یا شــرکای تجاری سازمان بگذارد. اطلاعات خصوصی کارکنان نیز شامل این طبقه‌بندی می‌شوند.

  - **محدود (Restricted)**

اطلاعات محدود، آن دسته از اطلاعات کسب‌وکار می‌باشند که در اختیار افراد مجاز محدودی در داخل و خارج ســازمان بوده و محافظت می‌گردند. افشــای غیرمجاز این نوع اطلاعات برخلاف خط‌مشــی امنیت اطلاعات بوده ولی انتظار نمی‌رود اثر مخربی روی کســب‌وکار، مشــتریان، کارکنان یا شــرکای تجاری سازمان بگذارد.

  - **عمومی (Public)**

اطلاعات عمومی، آن دسته از اطلاعات کسب‌وکار می‌باشند که می‌تواند در دسترس عموم قرار گیرد.

- **شخصی (Private)**

اطلاعات شخصی، آن دسته از اطلاعات کاملاً خصوصی کاربر و غیر سازمانی می‌باشند که سازمان در شرایط خاص و ممیزی‌ها اختیار دسترسی به آن‌ها را دارا می‌باشد ولی مجاز به افشای آن نیست.

- چنانچه در اسناد اشاره به اطلاعات حساس و حیاتی شده باشد منظور از آن اطلاعات محرمانه و یا در صورت وجود طبقات بالاتر می‌باشد.
- چنانچه مستندات شامل مجموعه‌ای از اطلاعات است که مشمول طبقه‌بندی متنوعی می‌گردند، نوع طبقه اطلاعات آن بایستی بر اساس بالاترین رده طبقه‌بندی آن مستند باشد. مثلاً اگر مستندی شامل اطلاعات "محدود" و "محرمانه" باشد، باید سطح طبقه آن "محرمانه" تعیین گردد.
- معیارهایی که در طبقه‌بندی اطلاعات تأثیرگذار هستند، شامل موارد زیر می‌باشند:

- ارزش اطلاعات
- حصول اطمینان از مناسب بودن سطح حفاظتی اطلاعات
- میزان خطری که به‌واسطه افشاء شدن اطلاعات متوجه سازمان می‌گردد.
- میزان خطری که به‌واسطه تغییر یا تحریف اطلاعات متوجه سازمان می‌گردد.
- میزان خطری که به‌واسطه در دسترس نبودن اطلاعات متوجه سازمان می‌گردد.
- میزان مسئولیت‌های قانونی، حقوقی یا قراردادی جهت محافظت از اطلاعات.

b. خط‌مشی‌های به‌کارگیری، نگهداری و مبادله اطلاعات

۱. کلیه افرادی که اطلاعات محرمانه روی رسانه‌های ذخیره‌سازی اطلاعات ازجمله لپ‌تاپ، فلش دیسک، سی‌دی، دی‌وی‌دی و ... دارند، مسئول حفظ و نگهداری امنیت این اطلاعات بوده و بایستی آن‌ها را رمزدار نمایند.
۲. درصورتی‌که اطلاعات محرمانه بر روی کامپیوترها، لپ‌تاپ‌ها، PDA و یا هر نوع سیستم دیگری ذخیره شود، نباید دستگاه را بدون قفل و یا خارج شدن از سیستم ترک کنند. به‌عبارت‌دیگر می‌بایست دسترسی به اطلاعات محرمانه را محدود سازند.
۳. اطلاعات محرمانه کاغذی باید به‌وسیله اشخاص قابل‌اطمینان ارسال گردیده و ارسال اطلاعات الکترونیکی نیز می‌بایست به آدرس پست الکترونیکی ثبت‌شده و مشخص انجام گردد و دیگر روش‌ها ازجمله پست‌های الکترونیکی‌ای که به‌صورت روتین زده می‌شوند ممنوع می‌باشند.

۴. در صورت نیاز به ارسال اطلاعات از طریق پست الکترونیکی، فقط باید از پست الکترونیکی تعریف‌شده سازمان به آدرس Username@mashhad.ir استفاده گردد.
۵. محافظت از اطلاعات در برابر دستبرد، نسخه‌برداری، تغییر و تخریب صورت پذیرد.
۶. کشف و محافظت در برابر کدهای مخرب و mobile code که ممکن است با استفاده از ارتباطات الکترونیکی منتقل می‌شود.
۷. محافظت از اطلاعات الکترونیکی حساس منتقل‌شده به شکل اطلاعات موردبحث و فایلهای Attache شده. ارجاع به سند email policy
۸. روش‌های رمزنگاری (برای حفاظت از محرمانگی، تمامیت و صحت اطلاعات) الزاماً باید اجرا شود (Cryptography)
۹. درصورتی‌که اطلاعات محرمانه از طریق پست‌های داخلی، خارجی و یا پیک‌ها ارسال می‌شوند، می‌بایست در دو پاکت و یا محفظه جداگانه قرار داده شوند. پاکت و یا محفظه خارجی نباید مشخص‌کننده نوع طبقه‌بندی و یا نوع اطلاعات موجود در آن باشد و از طرفی محفظه و یا پاکت داخلی الزاماً می‌بایست به روشی مناسب مهروموم گردد به‌صورتی که محتویات موجود در آن قابل‌رؤیت نبوده و دارای برچسب محرمانه باشد. پاکت‌ها و محفظه‌های محتوی اطلاعات محرمانه می‌بایست به نحوی علامت‌گذاری شده باشند تا آدرس و مشخصات شخص دریافت‌کننده و نیز نشانی فرستنده و دریافت‌کننده مرسوله کاملاً مشخص باشد. همچنین در صورت ارسال فایل‌های الکترونیکی، می‌بایست از طریق رمزگذاری مناسب (به‌طور نمونه استفاده از فایل‌های Zip شده دارای رمز عبور) نسبت به ارسال ایمن آن‌ها اطمینان حاصل نمایند.
۱۰. در تحویل کلیه اطلاعات محرمانه باید به‌گونه‌ای رفتار گردد که تأیید شخص گیرنده اطلاعات اخذ گردد. تحویل اطلاعات محرمانه به هر واسط دیگری به‌عنوان دریافت‌کننده ممنوع می‌باشد.
۱۱. کارکنان می‌بایستی از نمایش اطلاعات محرمانه و بحث و بررسی در مورد آن در مکان‌های عمومی خودداری نمایند.
۱۲. داده‌ها/اطلاعات کاغذی که حاوی اطلاعات محرمانه می‌باشند، بایستی به صورتی مطمئن در محلی به‌دوراز دسترسی غیرمجاز، حفظ و نگهداری گردند و در صورت عدم نیاز به این اطلاعات یا پس از استفاده، بایستی به شکلی امحاء گردند که امکان استفاده از آن برای افراد غیرمجاز میسر نگردد.
۱۳. افراد غیرمجاز اجازه دسترسی به اطلاعات محرمانه و محدود را ندارند.
۱۴. هیچ‌یک از کارکنان اجازه ندارند اطلاعات محرمانه و محدود سازمان را در اختیار افراد غیرمجاز قرار دهند.
۱۵. هر یک از کارکنان سازمان فاوا در صورتی‌که مواردی خلاف قانون، عرف یا سیاست‌های حرفه‌ای – سازمانی، مشاهده نمایند، بایستی ضمن حفظ محرمانگی و امنیت اطلاعات، مراتب را به مدیر خود گزارش نمایند.

۱۶. اطلاعات محرمانه نبایستی از طریق تلفن اطلاع‌رسانی شوند.
۱۷. هیچ‌یک از کارکنان اجازه ندارند اطلاعات محرمانه را روی تجهیزات چاپ مانند پرینتر، اسکنر، فکس و ... رها نمایند.
۱۸. داده‌ها/اطلاعات محرمانه روی نسخه‌های چاپی که اطلاعات مندرج در آن‌ها استفاده نخواهند شد، بایستی از طریق خرد و ریزریز کردن، منهدم شوند.
۱۹. در مواردیکه در حین همکاری با پیمانکاران/اشخاص ثالث، با اطلاعات محرمانه و محدود سازمان سروکار داشته باشیم، بایستی یک توافق‌نامه محرمانگی بین سازمان و آن‌ها منعقد گردد.
۲۰. اطلاعات محرمانه نباید به دستگاه فاکسی که مورد تأیید نمی‌باشد فرستاده شوند؛ به‌نوعی اطمینان حاصل شود که فرد مجاز بلافاصله اطلاعات فاکس شده را از روی دستگاه فاکس برداشته و در محل مناسبی حفظ و نگهداری خواهد نمود.
۲۱. اطلاعات محرمانه نباید از طریق بلندگو و یا speaker های تلفنی (SP-Phone) موردبحث و بررسی قرار گیرند، مگر آنکه کلیه افراد شرکت‌کننده در بحث، تأیید نمایند که اشخاص غیرمجاز در نزدیک و یا در مجاورت گفتگو، جهت استراق سمع حضور ندارند. کارکنان بایستی در خصوص اطلاعات محرمانه از پیغام گذاشتن بر روی منشی‌های تلفنی و یا سیستم‌های Voice Mail خودداری نمایند.
۲۲. تولیدکنندگان اطلاعات (مستندات، فایل‌های الکترونیکی و ...)، مالکان اطلاعات محسوب شده و مسئولیت تعیین نوع طبقه اطلاعات و برچسب‌گذاری اطلاعات با آن‌ها می‌باشد و در مورد اینکه، چه کسی یا کسانی برای دسترسی به اطلاعات مجاز می‌باشند و از چه اطلاعاتی می‌توانند استفاده نمایند، مدیر امنیت اطلاعات یا نماینده تام‌الاختیار وی تصمیم‌گیرنده است. مالکان اطلاعات باید تمهیداتی را به‌منظور اطمینان از اعمال کنترل های مناسب جهت نگهداری، مدیریت، توزیع و استفاده روتین و منظم از اطلاعات اتخاذ نمایند.

توضیح ۱: مالکان طبقه‌بندی اطلاعات (تولیدکنندگان اطلاعات)، صرفاً مسئول طبقه‌بندی اطلاعات و اعمال کنترل‌های لازم بوده و مالک قانونی اطلاعاتی که عهده‌دار نگهداری آن‌ها هستند نمی‌باشند، زیرا که آن‌ها توسط افراد ذیصلاح جهت نظارت و نگهداری از اطلاعات و سیاست‌های امنیتی مربوطه انتخاب گردیده‌اند.

برای فایل‌ها و مستندات الکترونیکی مهم، سازمان باید از سازوکاری برخوردار باشد که هویت ایجادکننده آن سند الکترونیکی قابل شناسایی باشد، همچنین باید لیستی از سوابق کلیه ویرایش‌ها و هویت ویرایش کننده برای آن اسناد در سیستم موجود باشد تا در موارد لزوم به آن مراجعه شود

۲۳. در صورتی‌که یکی از اتفاقات ذکر شده در ذیل برای اطلاعات محرمانه روی دهد، می‌بایست بلافاصله مالک آن اطلاعات یا مدیر مربوطه مطلع گردد:

- گم‌شدن، مغشوش شدن و یا از بین رفتن
- افشاء برای افراد یا طرف‌های غیرمجاز
- امکان افشاء برای افراد یا طرف‌های غیرمجاز
- عدم اطمینان از امحاء

۲۴. می‌بایست محیط ذخیره‌سازی حاوی اطلاعات در هنگام حمل‌ونقل خارج از مرزهای فیزیکی سازمان در برابر دسترسی غیرمجاز استفاده نابجا و یا صدمه محافظت شود.

۲۵. در خصوص مستندات وارده از سایر بخش‌های شهرداری مشهد، سازمان‌ها، شرکت‌ها و اشخاص ثالث به محدوده سیستم مدیریت امنیت اطلاعات، در صورت تعریف نشدن سطح طبقه مناسب از سوی ارسال‌کننده، اولین مقام ذیصلاح دریافت‌کننده مستند، می‌بایست نسبت به انتخاب سطح طبقه‌بندی مناسب جهت آن مستند اقدام نموده و مطابق با مستندات داخلی طبقه‌بندی‌شده با آن برخورد نماید.

۲۶. اطلاعات در صورتی در معرض دید عموم قرار می‌گیرند که قبلاً مجوز کتبی آن توسط دبیر کمیته راهبری صادرشده باشد. همچنین این اطلاعات می‌بایستی در برابر تحریف اطلاعات محافظت گردند.

۲۷. قابل‌توجه می‌باشد که اطلاعاتی که پس از یک دوره زمانی در معرض عموم قرار می‌گیرد دیگر حساس و حیاتی قلمداد نمی‌رود.

c. خط‌مشی‌های برچسب‌گذاری اطلاعات

رویه‌های برچسب‌زنی اطلاعات، شامل اطلاعات در قالب فیزیکی و الکترونیکی می‌باشد.

الف- برچسب‌گذاری اطلاعات الکترونیکی (فایل‌های الکترونیکی)

در خصوص اطلاعاتی که از نوع الکترونیکی می‌باشند، برچسب‌گذاری از طریق درج حرف اول نوع طبقه اطلاعات به زبان انگلیسی،{(C) = Confidential (R) = Restricted, (P) = Public} پس از نام فایل، روی آیکون فایل (File Icon) مربوطه صورت می‌گیرد. علاوه بر این بایستی در Footer تمامی صفحات فایل‌هایی که از نوع Microsoft Office Word Document می‌باشند، نوع طبقه اطلاعات به زبان انگلیسی با فونت Times New Romanبا سایز ۱۲ در گوشه سمت چپ پایین صفحات درج گردد.

ب- برچسب‌گذاری اطلاعات و مستندات کاغذی

اطلاعات و مستندات کاغذی چاپی که مطابق با روش بالا (الف. اطلاعات الکترونیکی) برچسب‌گذاری نشده‌اند، شامل موارد ذیل می‌باشند:

۱. انواع اطلاعات و مستندات کاغذی چاپی که قبلاً در شهرداری مشهد تهیه‌شده‌اند.

۲. مستندات کاغذی چاپی وارده از سایر سازمان‌ها، شرکت‌ها و اشخاص ثالث به شهرداری مشهد در مورد این نوع از اطلاعات، درصورتی‌که از نوع «محرمانه» باشند، روی تمامی صفحات آن‌ها مهر «محرمانه» به رنگ قرمز و درصورتی‌که از نوع «محدود» باشند، روی تمامی صفحات آن‌ها مهر «محدود» به رنگ آبی درج می‌گردد.

ج- برچسب‌گذاری رسانه‌های ذخیره‌سازی اطلاعات

کلیه رسانه‌های حاوی اطلاعات طبقه‌بندی‌شده، شامل نوارها (Tapes)، دیسک‌ها، CD&DVD ها و ...، بایستی با توجه به نوع اطلاعات ذخیره‌شده در آن‌ها برچسب‌گذاری گردند. درصورتی‌که انواع طبقات اطلاعات، در این رسانه‌ها ذخیره‌شده باشد، مطابق با خط‌مشی شماره ۳ بند ۱,۴. همین سند اقدام می‌گردد.

د- برچسب‌گذاری ایمیل‌های سازمانی

در Subject کلیه ایمیل‌های سازمانی، بایستی نوع طبقه اطلاعات مندرج در آن به زبان انگلیسی پس از عنوان ایمیل مربوطه داخل پرانتز درج گردد؛ یعنی (Confidential) برای اطلاعات از نوع محرمانه، (Restricted) برای اطلاعات از نوع محدود و (Public) برای اطلاعات از نوع عمومی پس از عنوان ایمیل مربوطه درج گردد.

- مستندات فاقد برچسب طبقه‌بندی اطلاعات به‌صورت پیش‌فرض در پایین‌ترین سطح طبقه‌بندی اطلاعات (اطلاعات عمومی) قرار خواهند گرفت.

تغییر طبقه اطلاعات

۱. حساسیت و ارزش اطلاعاتی که پس از یک دوره زمانی خاص تغییر می‌کنند، بایستی توسط مالک داده‌ها/اطلاعات موردبازنگری قرارگرفته و مجدداً طبقه‌بندی گردند تا درجه طبقه‌بندی جدید آن‌ها مشخص گردد. بااین‌حال بایستی حداقل سالی یک‌بار مالکان اطلاعات نسبت به بازنگری طبقه‌بندی اطلاعات اقدام نمایند.

۲. در صورت تغییر طبقه اطلاعات، مالک اطلاعات بایستی موارد ذیل را انجام دهند:

الف- برچسب طبقه اطلاعات را بر روی نسخه اصلی اطلاعات تغییر دهد.

ب- تمامی متولیان و دریافت‌کنندگان اطلاعات را که سابقاً مشخص‌شده‌اند، از این تغییرات به نحوی مطلع سازد.

ج- تغییرات را به اطلاع واحد و یا اشخاص متولی بایگانی و یا نگهداری اطلاعات برساند.

اقدامات انضباطی:

هرگاه یکی از کاربران اقدام به نقض این ســـند نماید، مطابق با آیین‌نامه انضـــباطی با وی برخورد خواهد شد.

دوره بازنگری:

این ســند و همه ضــمایم آن، حداقل ســالی یک‌بار و در مواردی که موردنیاز می‌باشــد، موردبازنگری قرار می‌گیرد.

مراجع و ضمایم:

راهنمای استفاده از آئین‌نامه و پیوست شماره ۱

پیوست ۱

نحوه نگهداری تجهیزات و اطلاعات

- از آنجائیکه تجهیزات کامپیوتری بطور روزمره توسط کاربران متعدد در حال استفاده هستند، لذا با توجه به وجود غبار و آلودگی‌های محیطی به مرور کثیف شده و چنانچه نگهداری مناسبی در خصوص آنها صورت نپذیرد، غیرقابل استفاده می‌گردند. لذا حتما توصیه می شود در بازه‌های زمانی مابین سرویس‌های دوره‌ای نسبت به نگهداری تمیز و صحیح تجهیزات مانند صفحه نمایش، صفحه کلید و ماوس مبادرت گردد.
- کلیه سیمها و کابل‌های مورد استفاده در ارتباطات سخت‌افزاری مانند کابل مانیتور، صفحه کلید، ماوس و شبکه بطور منظم و دقیق جمع‌آوری شده و حتی‌الامکان دارای سیم‌زیپ باشند.
- در خصوص نحوه کار با سیستم عامل و کلیه نرم‌افزارهای پایه‌ای و کاربردی آشنایی حداقلی وجود داشته باشد. در این خصوص لازم است تا کلیه همکاران محترم شهرداری که به واسطه نوع کارهای محوله بایستی با انواع نرم‌افزارهای مختلف سروکار داشته باشند، قبل از مبادرت به شروع کار حتما نسبت به آشنایی حداقلی (در سطح کاربری متعارف) با آن نرم‌افزار مبادرت ورزند. بدیهی است گذراندن دوره آموزشی، مطالعه مستندات و راهنمای کاربری و مشاهده فیلمهای آموزشی تخصصی اقدام نمایند.
- در خصوص ذخیره و نگهداری فایل‌های جاری و روزمره، دانلود پیوست‌های ایمیل و نیز نگهداری فایل‌های دریافتی از نرم‌افزارهایی همچون Lync و Jabber می‌بایست از فضاهای دیسک سخت بجز درایو سیستم عامل (C) و یا فضای میزکار (Desktop) استفاده گردد. در این خصوص می‌توان از روش میان‌بر (Shortcut) برای موارد ضروری استفاده گردد.
- همانگونه که در بخش اصلی آئین‌نامه هم ذکر گردیده است به منظور سامان‌دهی و دسته‌بندی اطلاعات میبایست از روش پوشه‌بندی و لیبل‌گذاری آنها استفاده نمود. در این خصوص توضیحات کافی در بند C تحت عنوان **خط‌مشی‌های برچسب‌گذاری اطلاعات** بطور کامل آموزش داده شده است.
- از آنجائیکه بسیاری از سرویس‌های متداول در حوزه فناوری اطلاعات در شهرداری مشهد بومی‌سازی شده است لذا انتظار می‌رود کلیه کاربران نسبت به استفاده از آنها مبادرت ورزند. در این خصوص سرویس‌های پایه‌ای همچون پست الکترونیک، نرم‌افزارهای گپ و گفتگو معروف به Lync و نیز Jabber پیشنهاد می‌گردند. بدیهی است جزوات راهبری و نحوه استفاده از هرکدام قابل دسترسی است.
- ارتباط آدمی با ابزار و وسایلی که در زندگی روزمره مورد استفاده قرار می دهد تاثیر آشکاری بر سلامتی او دارند . تجهیزات جانبی رایانه ها که امروز جایگاه خاصی را در زندگی روزانه انسان به

خود اختصــاص داده اند نیز از این امر مســتثنی نخواهند بود . لذا در خصــوص مواردی همچون محیط کار، نور، میز، صندلی و ارتفاع هرکدام بایستی استانداردهای لازم ارگونومی محیط کار را داشته باشند.

- وجود و صحت کارکرد نرم‌افزار آنتی‌ویروس حتما بایستی چک شود و بروزبودن آن بطور روزانه مورد بازدید قرار گیرد.