منشور سازمانی
رویه های اجرایی
"حفظ محرمانگی اطلاعات نهانی و داده های الکترونیکی"

شرکت زرین معدن آسیا (سهامی عام)

	تهیه کننده	تصویب کننده
سمت	مدیر واحد فناوری اطلاعات IT	مدیر عامل
نام و نام خانوادگی	مهندس سعید علیمی	مهندس شهرام کدخدائی
امضاء		

تذکر :
اسناد سیستم مدیریت یکپارچه (IMS) و روش اجرایی محرمانگی داده الکترونیکی
فقط با مهر اصلی دارای اعتبار میباشد و تهیه کپی از اسناد مجاز نیست.

مهر کنترل

شرکت زرین معدن آسیا (سهامی عام) شماره ثبت ۶۲۸۵

۱ -اهداف

این روش اجرایی با هدف **حفظ امنیت و صحت اطلاعات، استفاده صحیح از امکانات سخت‌افزاری و نرم‌افزاری** و همچنین **حصول اطمینان از پایداری شبکه** از لحاظ ارتباطات، تهیه و تدوین گردیده است.

امنیت اطلاعات :شامل محرمانگی، حفظ صحت و یکپارچگی، و دسترس‌پذیری در زمان ایجاد، انتقال و نگهداری است.

۲ -دامنه کاربرد

این روش اجرایی شامل کلیه اطلاعات سازمان (اعم از اطلاعات داخل شرکت و اطلاعات مربوط به کارفرمایان)، سیستم‌های کامپیوتری و تجهیزاتی است که به شبکه متصل و درون سازمان قرار دارند. همچنین، سیستم‌هایی که با نام سازمان در خارج از شرکت (مانند پروژه‌ها) و کلیه کاربران داخلی و خارجی شبکه که با سیستم‌های سازمان درگیر هستند را نیز در بر می‌گیرد.

۳ -تعاریف

- **اطلاعات :**داده‌های پردازش شده که شامل تمامی اطلاعات دیجیتالی مبنایی برای تصمیم‌گیری می‌باشند. اطلاعات یک دارایی است که همانند سایر دارایی‌ها باید حفظ و نگهداری شود.
- **اطلاعات شامل :**متون، نقشه‌ها، تصاویر، نامه‌ها، پرونده‌ها، اسناد، فایل‌های کامپیوتری، اطلاعات توصیفی و جغرافیایی و ...، چه در داخل شبکه و سرورها و چه بر روی کلاینت‌ها و کامپیوترهای مستقل. همچنین مستندات الکترونیکی، مراسلات متداول، رسانه‌های الکترونیکی، سوابق پایگاه داده، ایمیل‌ها، نوارها، DVDها، CDها، فیلم‌ها و اطلاعات بیان شده در جلسات.
- **کاربران :**شامل کارکنان، پیمانکاران مرتبط با شبکه و سایر کاربرانی که به نحوی با بخش‌های مدیریتی یا کاربردی درون سازمانی شبکه در ارتباط می‌باشند.
- **نرم‌افزار :**شامل سیستم‌عامل‌ها مانند Linux ، Windows، نرم‌افزارهای کاربردی عمومی (مانند Office، نرم‌افزارهای کاربردی سازمانی (مانند سیستم اتوماسیون اداری)، نرم‌افزارهای کاربردی اختصاصی

(مانند سیستم‌های فنی و مهندسی)، نرم‌افزارهای مدیریت شبکه و سیستم‌های تحت وب) مانند File Server، My SQL Server، SQL Server، Email Server، Active Directoryو.(...

- **سخت‌افزار** :شامل ایستگاه‌های کاری، سرویس‌دهنده‌ها، Data Projectorها، PCها، Laptopها، تجهیزات شبکه و انتقال داده) مانندRouter ها، Switchها، Hubها(، چاپگرها، پویشگرها، و تجهیزات سیار انتقال اطلاعات) مانندFlash Memory ها، CDها، DVDها، دوربین‌های دیجیتالی و.(...
- **ارتباطات** :شامل کابل‌های فیبرنوری، CAT6وCAT7 ، ارتباطات شبکه سازمان با سایر شبکه‌های موجود (مانند شبکه سایر کارخانجات و دفتر مرکزی)، شبکه اینترنت و....
- **کاربر مجاز** :کاربرانی که با تأیید بخش اداری و توجه به پروسه جذب در سازمان احراز هویت گردیده‌اند و دارای نام کاربری در دامنه سازمان می‌باشند.
- **کاربر مجاز موقت** :کاربرانی که با تأیید مدیر قسمت و بدون توجه به پروسه جذب در سازمان، نیاز به استفاده از نام کاربری موقت در دامنه سازمان را دارند.
- **کاربران خارجی** :کاربرانی که از سازمان‌های بیرونی به سازمان سرویس می‌دهند.
- **سیستم PAM (Privileged Access Management):** سیستم مدیریت دسترسی‌های ممتاز، ابزاری که برای کنترل، پایش و ضبط کلیه جلسات دسترسی کاربران ممتاز به منابع حساس شبکه (مانند سرورها، تجهیزات شبکه و دیتابیس‌ها) استفاده می‌شود.
- **پورتال سازمانی** :هرگونه سامانه یا نرم‌افزار تحت وب که برای تسهیل امور داخلی سازمان) مانند اتوماسیون اداری، پورتال منابع انسانی، Intranet، مدیریت پروژه‌ها (طراحی شده و صرفاً توسط کارکنان یا کاربران مجاز داخلی مورد استفاده قرار می‌گیرد.

۴ -مسئولیت نظارت و اجرا

- **مدیر عامل** :مسئول تصویب و ابلاغ روش اجرایی امنیت اطلاعات به همه واحدهای شرکت است.
- **مدیر واحد فناوری اطلاعات و ارتباطات** :مسئول تدوین، به‌روزآوری، نظارت بر حُسن اجرای این روش اجرایی در واحد فناوری اطلاعات و کلیه واحدهای سازمان و همچنین بازنگری و بهبود آن در مقاطع مقتضی است. همچنین مسئولیت مدیریت فنی سایت شرکت و زیرساخت‌های پورتال‌ها را دارا است.
- **معاونین و مدیران واحدها** :مسئول نظارت بر حُسن اجرای روش اجرایی در واحد تحت مدیریت خود هستند.
- **مدیران پروژه‌ها** :مسئول اجرای روش اجرایی در تمام مقاطع اجرای پروژه‌ای که مدیریت آن را بر عهده دارند، و در تمام واحدهای درگیر هستند.

- **کاربران :**مسئول اجرای روش اجرایی هستند.
- **مدیر سیستم‌ها و روش‌ها :**مسئول پایش روش اجرایی و گزارش آن به مدیر عامل در مقاطع مقتضی است.
- **مشاور انفورماتیک :**مسئول همکاری با مدیر واحد فناوری اطلاعات در پیاده‌سازی و انتخاب سخت‌افزار و نرم‌افزار مناسب و همچنین ارائه پیشنهادات بهبود است.
- **مدیر توسعه بازار/واحد محتوا :**مسئول مدیریت و تأیید صحت محتوای منتشر شده در وب‌سایت رسمی شرکت است.

۵ -شرح رویه‌های اجرایی

- اطلاعات سازمان صرفاً توسط افراد مجاز قابل دسترسی باشند.
- محرمانگی اطلاعات می‌بایست همواره در کل شرکت، در پروژه‌ها و بین واحدهای سازمانی حفظ شود.
- در کلیه فرایندهای امنیتی، یکپارچگی اطلاعات حفظ گردد.
- پیاده‌سازی سیاست‌های امنیتی نباید اختلالی در روند کاری سازمان و واحدها ایجاد کند.
- آموزش‌های لازم در مورد امنیت اطلاعات و سیاست‌های امنیتی مربوط به کل سازمان است.
- تمامی رخنه های امنیت اطلاعات و ضعف‌های احتمالی باید توسط همه کاربران گزارش شده و به آنها رسیدگی گردد.
- تبادل اطلاعات بین سازمانی همواره باید از طریق کانال‌های مجاز و مورد تأیید سازمان صورت گیرد.
- تمام دستورالعمل‌های امنیتی مصوب برای کلیه سازمان یکسان است و موارد استثنا، تنها در صورت دستور کتبی مدیریت ارشد اعمال می‌شود.
- هرگونه خارج نمودن و انتشار اطلاعات شرکت، مگر با اخذ مجوز از مقامات ذیصلاح، تخلف محسوب می‌شود.
- کلیه نرم‌افزارهای داخلی که از طریق آنها تولید محتوا می‌شود، باید مشخص، استانداردسازی و منطبق بر سیاست‌های امنیتی سازمان به‌کار رود.
- هر کاربر در شبکه فقط مجاز است به اطلاعاتی دسترسی داشته باشد که از طرف مدیران مافوق برای او مجاز است. هرگونه تلاش برای دسترسی به اطلاعاتی خارج از حیطه (اعم از مشاهده، تغییر، دستکاری و ...) اکیداً ممنوع و تخلف محسوب می‌شود.
- اختلال در عملکرد شبکه و کاربران اکیداً ممنوع است. از اقداماتی که منجر به تخریب اطلاعات شود، پرهیز شود.
- هرگونه تلاش جهت نفوذ به سایر کلاینت‌ها، سرورها و دیتابیس‌ها، که جزء دسترسی مجاز یک کاربر نمی‌باشد، با هرگونه ابزار سخت‌افزاری یا نرم‌افزاری، تخلف محسوب می‌شود.

در راستای اجرای دقیق این روش اجرایی، موارد به شرح زیر طبقه‌بندی می‌گردد:

۵-۱ -پست الکترونیکی

- ۵-۱-۱ -ایمیل‌های سازمانی: معرفی و ایجاد ایمیل‌های سازمانی توسط کارشناسان IT با نظر مدیران هر واحد انجام می‌شود.
- ۵-۱-۲ -ایمیل‌های شخصی: استفاده متعارف از منابع سازمان برای ایمیل‌های شخصی پذیرفتنی است، ولی ایمیل‌های غیرمرتبط با کار می‌بایست در پوشه جداگانه و مجزا از ایمیل‌های کاری نگهداری شوند. در ضمن ایمیل‌های شخصی باید از ایمیل‌های سازمانی جدا شوند.
- کارکنان سازمان نباید انتظار داشته باشند پیام‌هایی که در سیستم پست الکترونیکی سازمان ذخیره، ارسال و دریافت می‌کنند، در قالب حیطه شخصی آنها تلقی و محرمانه باشد. سازمان ممکن است بدون هشدار قبلی به نظارت و بررسی ایمیل‌ها بپردازد.
- فایل نگهداری ایمیل‌های سازمانی تنها در دسترس خود کاربر و کارشناس IT می‌باشد.
- تمامی ایمیل‌هایی که حاوی اطلاعات سازمانی هستند، به‌طور روزانه نسخه پشتیبان تهیه و در سرور نگهداری شوند.
- ارسال ایمیل سازمانی برای خارج از شرکت (اعم از کارفرمایان، تأمین‌کنندگان و سایر اشخاص حقیقی) تنها توسط مدیران و پست‌های سازمانی معرفی شده توسط ایشان انجام شود. لیست تأییدیه افراد مجاز نزد واحد فناوری اطلاعات شرکت نگهداری شود.

۵-۲ -اطلاعات ذخیره شده در سرور

- ۵-۲-۱ -اطلاعات سازمانی: این اطلاعات اهمیت بسیار زیادی در سازمان دارد. اطلاعات این قسمت توسط مدیران هر واحد مشخص خواهد شد. بر طبق چارت سازمانی، دسترسی هر شخص توسط مدیر همان قسمت به اطلاعات مشخص خواهد شد. از قرار دادن اطلاعات شخصی در این قسمت باید خودداری شود.
- ۵-۲-۲ -اطلاعات فردی: کلیه اطلاعات کاربران سازمان روی سرور ذخیره می‌شود. اطلاعات فردی در **درایو D**هر سیستم قابل مشاهده است.
  - کاربران از قرار دادن اطلاعات سازمانی در **درایو D** خودداری کنند.
  - اطلاعاتی که کاملاً شخصی است، نباید در سیستم نگهداری شود.
  - مسئولیت پاک شدن اطلاعات فردی بر عهده کاربر است.
  - قرار دادن فایل‌های Multi Media و عکس در **درایو D** امکان‌پذیر نمی‌باشد.
  - مدیران هر واحد باید دسته‌بندی منظم و دقیقی را برای حفظ و نگهداری اطلاعات به‌منظور دسترسی سریع ایجاد کنند و کلیه کاربران موظف به رعایت آن هستند.
  - کلیه فایل‌های مهم باید رمز عبور داشته باشند.

۵-۳ -نرم‌افزار ERP

- نرم‌افزار ERP شامل سیستم‌های مالی، منابع انسانی، انبار، حقوق و دستمزد، اموال و ... دارای زیرسیستم‌های مختلفی است. کاربر هر واحد با توجه به مجوز صادره از طریق معاونت اداری و مالی به آن دسترسی دارد.
- این نرم‌افزار دارای سطوح دسترسی مختلفی است. مسئولیت اجرای مجوز به عهده مدیر واحد فناوری اطلاعات است.
- کلیه اطلاعات این نرم‌افزار بر روی سرور نگهداری شود.
- در صورت لزوم، تبادل اطلاعات (رپلیکیشن بین سرورها) بین سرورهای دفتر مرکزی جهت به‌روزرسانی اطلاعات مربوط به سیستم ERP و پروژه‌های سازمان انجام شود.
- هر کاربر با نام کاربری و رمز عبور خود وارد سیستم می‌شود و مسئولیت نگهداری و تغییر کلمه عبور بر عهده کاربر است.
- مدیریت تبادل اطلاعات بین سرورها بر عهده مدیر IT است.
- کارکرد درست روترها و رپلیکیشن به‌منظور برقرای درست ارتباط به‌طور مستمر باید کنترل و چک شود.
- دستورات پینگ برای ارتباط با روتر دفتر مرکزی و پروژه‌ها و شرکت‌های مشارکت کننده باید کنترل شود.
- در صورت قطع شدن ارتباط، تمامی آدرس‌های IP ارتباط بین دو نقطه کنترل می‌شود.

۵-۴ -اطلاعات مربوط به Active Directory

- تعریف/حذف کاربران و رمزهای کاربران، اطلاعات مربوط به پروفایل‌های آنها، ایجاد دسترسی‌ها و مدیریت سرورDNS ، DHCPبر عهده مدیر واحد فناوری اطلاعات است.
- ۵-۴-۱ -رمز عبور:
  - رمز عبور هر کاربر باید تقریباً هر **۴ هفته** یک‌بار تغییر کند.
  - در هنگام فاش شدن رمز عبور، کاربر باید در سریع‌ترین زمان ممکن رمز عبور خود را تغییر دهد.
  - کاربران اجازه واگذاری نام کاربری و رمز عبور خود به دیگران را ندارند.
  - رمز عبور کاربران باید حداقل از **۱۰حرف** تشکیل شده باشد.
  - در رمز عبور باید حداقل دو تا از کاراکترهای حرفی وجود داشته باشد.
  - در رمز عبور نباید از حروف یا اعداد پشت سر هم استفاده شود) مانند qwerty یا ۱۲۳۴۵.(
  - در رمز عبور نباید از نام یا نام خانوادگی فرد استفاده شود.
  - تغییر در رمز عبور باید به اطلاع مدیر مستقیم کاربر برسد.
  - **رمز عبور کاربر نمی‌تواند برای حداقل ۳ دوره قبل استفاده گردد.**
- ۵-۴-۲ -ایجاد و مدیریت دسترسی کاربران:
  - کلیه دسترسی‌ها به اطلاعات مرتبط با حوزه کاری کاربر باید با درخواست مستند پس از تأیید توسط مدیر مستقیم ایجاد شوند.

- کلیه دسترسی‌ها به اطلاعات غیرمرتبط با حوزه کاری کاربر باید با درخواست مستند پس از تأیید توسط مدیر مستقیم و معاونت اداری و مالی ایجاد شوند. بدیهی است که درخواست‌های تأیید شده توسط مدیر عامل، لازم‌الاجرا هستند.
- کلیه کاربران سازمان باید بخشنامه قوانین امنیت اطلاعات سازمان را مطالعه و امضاء کرده باشند.
- کلیه اسامی کاربری در سیستم می‌بایست به صورت منحصر به فرد ایجاد شوند.
- کاربرانی که بیش از ۱۰ روز از کد کاربری خود استفاده نکنند، غیرفعال می‌شوند.
- مراحل ایجاد و تغییر کاربران باید مستند شود و در دوره‌های زمانی مشخص مورد بازبینی قرار گیرند.
- کاربرانی که از مجموعه جدا و یا به هر دلیلی قطع همکاری با سازمان دارند، باید نام کاربریشان در سیستم به مدت دو ماه غیرفعال و پس از آن حذف شود.
- کلیه تعاریف حق دسترسی باید توسط واحد فناوری اطلاعات کنترل و اجرا شود.

۵-۵ -مدیریت محتوا، طراحی و انتشار وب‌سایت

در راستای حفظ اعتبار سازمان و اطمینان از صحت اطلاعات منتشر شده:

- **مالکیت و مسئولیت محتوا :**کلیه محتوا و داده‌های منتشر شده در وب‌سایت سازمان (شامل متن، تصاویر، طراحی، کد) دارایی سازمان محسوب می‌شود. مسئولیت تأیید صحت، به‌روز بودن و انطباق قانونی محتوای منتشر شده مستقیماً بر عهده **مدیر توسعه بازار/واحد محتوا** است.
- **استانداردهای طراحی و برندینگ :**تمامی طرح‌ها و قالب‌های بصری وب‌سایت باید با استانداردهای رسمی برندینگ و هویت سازمانی تطابق داشته باشند.
- **فرآیند تولید و تأیید :**تولید و انتشار هرگونه محتوای جدید یا تغییرات عمده در سایت باید پس از اخذ تأییدیه کتبی نهایی از **مدیر توسعه بازار/واحد محتوا** صورت گیرد.
- **محیط آزمایشی :(Staging)** کلیه تغییرات ساختاری، طراحی و محتوایی عمده باید قبل از انتشار در محیط اصلی(Production) ، ابتدا در یک محیط آزمایشی امن (Staging Environment) پیاده‌سازی، تست و تأیید شوند.
- **کیفیت و :SEO** محتوا باید با هدف افزایش اعتبار سازمانی، رعایت اصول فنی سئو و بهبود رتبه‌بندی در موتورهای جستجو تولید و به‌طور مستمر پایش شود.

۵-۶ -امنیت زیرساخت وب، دامنه و هاستینگ

به منظور محافظت از زیرساخت‌های اینترنتی سازمان در برابر حملات و دسترسی‌های غیرمجاز:

- **مدیریت زیرساخت :**مدیریت ثبت، تمدید دامنه، تنظیمات DNS و کنترل پنل هاستینگ (شامل دسترسی به پایگاه داده و فایل‌ها) صرفاً بر عهده واحد **فناوری اطلاعات و ارتباطات** است.
- **رمزنگاری ترافیک :(HTTPS)** استفاده از گواهی‌های معتبر SSL/TLS و رمزنگاری تمامی ترافیک ورودی و خروجی وب‌سایت (HTTPS) الزامی است.
- **حفاظت و به‌روزرسانی پلتفرم :**به‌روزرسانی‌های امنیتی سیستم مدیریت محتوا(CMS) ، افزونه‌ها (Plugins)، کتابخانه‌ها و سیستم عامل سرور میزبان باید به‌طور منظم و فوری توسط واحد IT انجام پذیرد.
- **فایروال نرم‌افزار وب :(WAF)** جهت جلوگیری از حملات متداول وب) مانند SQL Injection و (XSS، نصب و فعال‌سازی یک فایروال نرم‌افزار وب (WAF) یا ابزار امنیتی معادل در لایه دسترسی الزامی است.
- **دسترسی‌های ممتاز :**دسترسی به پنل‌های مدیریتی سطح بالا) مانند (SSH, Plesk/FTP/Database باید با رمزهای بسیار قوی، احراز هویت دومرحله‌ای (2FA) و محدود به آدرس‌های IP مجاز سازمان باشد.

۷-۵ -نگهداری و امنیت پورتال‌های سازمانی

این دستورالعمل برای حفظ امنیت سامانه‌ها و نرم‌افزارهای تحت وب داخلی(Intranet) ، پورتال HR ، سیستم مدیریت پروژه‌ها، امور سهام، تدارکات و (...اعمال می‌شود:

- **جداسازی شبکه :**پورتال‌های سازمانی باید به لحاظ فیزیکی یا منطقی) با استفاده از (VLAN از شبکه عمومی و وب‌سایت رسمی سازمان جدا شوند و دسترسی به آن‌ها فقط از طریق شبکه داخلی سازمان یا بستر **VPN/PAM**مجاز است.
- **احراز هویت کاربران :**احراز هویت کاربران پورتال‌ها باید ترجیحاً از طریق سیستم Active Directory سازمان Single Sign-On) یا (SSO صورت پذیرد. در غیر این صورت، استفاده از کلمات عبور قوی و احراز هویت دومرحله‌ای الزامی است.
- **کنترل دسترسی مبتنی بر نقش :(RBAC)** سطوح دسترسی کاربران به پورتال‌ها باید کاملاً مبتنی بر نقش‌های سازمانی آن‌ها بوده و با تأیید مدیر واحد مربوطه تنظیم شود.
- **بروزرسانی و تست آسیب‌پذیری :**به‌روزرسانی منظم سیستم‌عامل، دیتابیس و کدهای پورتال‌های سازمانی توسط واحد IT انجام شود. تست‌های دوره‌ای ارزیابی آسیب‌پذیری (Vulnerability Assessment) و نفوذپذیری (Penetration Testing) باید بر روی این سامانه‌ها اجرا شود.
- **پایش لاگ :**کلیه لاگ‌های دسترسی، خطاها و فعالیت‌های مدیران سیستم در پورتال‌ها باید به‌طور مستمر پایش و برای مدت حداقل ۶ ماه نگهداری شوند.

۵-۸ -اطلاعات مربوط به ورود و خروج در نرم‌افزار راهکاران(ERP)

- این نرم‌افزار جهت ثبت ورود و خروج کاربران استفاده می‌شود. واحد اداری مسئولیت استفاده از این نرم‌افزار را دارد.
- واحد فناوری اطلاعات وظیفه ایجاد امنیت براساس این روش اجرایی را برای اطلاعات این سیستم بر عهده دارد.
- نام کاربری و رمز عبور توسط کارشناس واحد فناوری اطلاعات ثبت و دسترسی‌های لازم به پرسنل داده شود.
- دسترسی کامل به این برنامه تنها در اختیار مسئول اداری و دسترسی مدیران سایر واحدها در حد مشاهده کارکرد پرسنل زیرمجموعه است.

۵-۹ -اینترنت

- اینترنت در سازمان در جهت به دست آوردن اطلاعات مفید و سودمند در جهت بهبود انجام مسئولیت، ارسال ایمیل و ... استفاده شود.
- مدیر هر واحد، میزان استفاده از اینترنت توسط کارکنان آن واحد را مشخص می‌کند.
- استفاده از اینترنت برای انجام کار شخصی ممنوع است.
- نصب و به‌کارگیری نرم‌افزارهایی که به اینترنت نیاز دارند باید با مجوز مدیریت هر دپارتمان انجام شود.
- میزان استفاده کاربران از اینترنت به‌طور ماهانه به مدیریت ارشد گزارش شود.
- هر کاربر تنها با نام کاربری و کلمه عبور خود می‌تواند وارد اینترنت شود.
- رمز وایرلس فقط در اختیار مدیران قرار دارد. فقط با تعریف مک آدرس یک دستگاه همراه امکان اتصال به وایرلس وجود دارد.
- سایر کاربران در سازمان مجاز به استفاده از شبکه وایرلس نمی‌باشند، مگر با تشخیص مدیریت واحد و به‌صورت محدود در زمان معین (این زمان بیشتر از مدت یک روز کاری نمی‌تواند باشد).
- کاربران مجاز به استفاده از اینترنت وایرلس حق انتقال رمز را به سایر کارکنان ندارند.
- در صورت به‌کارگیری اینترنت وایرلس، با توجه به محرمانگی اطلاعات، ورود به شبکه تحت هیچ شرایطی امکان‌پذیر نمی‌باشد.

۵-۱۰ -حفاظت در برابر ویروس‌ها و باج افزارها

- این بخش کلیه افرادی را که از منابع اطلاعاتی سازمان استفاده می‌کنند، در بر می‌گیرد.
- به‌منظور جلوگیری از ورود و همچنین شناسایی و مقابله با ویروس‌ها، کِرم‌ها و اسب‌های تروجان و ... از نرم‌افزار **Kaspersky** استفاده می‌شود. این نرم‌افزار روزانه از اینترنت به‌روزرسانی خواهد شد.

- کلیه کامپیوترهایی که به سازمان تعلق دارند یا توسط سازمان مدیریت می‌شوند، همین‌طور لپ تاپ‌هایی که به شبکه سازمان متصل می‌شوند یا به‌صورت مستقل مورد استفاده قرار می‌گیرند، می‌بایست از نرم‌افزار آنتی‌ویروس و تنظیمات مورد تأیید واحد فناوری اطلاعات سازمان استفاده کنند.
- تمامی کامپیوترهایی که به سازمان تعلق ندارند یا تحت مدیریت سازمان نمی‌باشند، پیش از هرگونه ارتباط و اتصال به منابع اطلاعاتی سازمان، باید از نرم‌افزار ضد ویروس و تنظیمات مورد تأیید مدیر واحد فناوری اطلاعات سازمان استفاده کنند.
- نرم‌افزار ضد ویروس نباید غیرفعال (Disable) شود. دسترسی کاربران به این گزینه امکان‌پذیر نیست.
- تنظیمات نرم‌افزار ضد ویروس نباید به‌گونه‌ای تغییر کند که قابلیت تأثیرگذاری آن را کاهش دهد.
- تنظیمات به‌روزرسانی نرم‌افزار ضد ویروس نباید به‌گونه‌ای تغییر کند که بازه‌های زمانی به‌روزرسانی آن را کاهش دهد.
- هر سرویس‌دهنده‌ای که به شبکه سازمان متصل است، باید از نرم‌افزار ضد ویروس مورد تأیید سازمان استفاده کند.
- تمام گذرگاه‌های پست الکترونیکی باید از نرم‌افزار ضد ویروس مورد تأیید سازمان استفاده کنند و تمامی نامه‌های ورودی و خروجی می‌باید توسط این نرم‌افزار کنترل شوند.
- هر ویروسی که به‌صورت خودکار توسط نرم‌افزار پاک نشود، باید در اولین زمان ممکن به واحد فناوری اطلاعات گزارش شود.
- کارشناس واحد فناوری اطلاعات باید به‌روزرسانی آنتی‌ویروس را چک کند و در صورت مشکل باید با شرکت موردنظر تماس برقرار کند.

۵-۱۱ -اطلاعات دوربین‌ها

- مدیریت و کنترل دوربین‌ها و کلیه اطلاعات مربوط به نرم‌افزار دوربین‌ها (شامل نام کاربری، کلمه عبور، نرم‌افزار نصب) و همچنین معرفی کاربرانی که مجاز به دیدن فیلم‌ها هستند، با واحد فناوری اطلاعات است.
- نرم‌افزار دوربین‌ها حتماً باید در سرور و نسخه کلاینت آن در کامپیوترهای کاربران مجاز نصب شود.
- فیلم ضبط شده دوربین‌ها باید در سرور نگهداری شود و این اطلاعات ذخیره شده باید چک شود.
- فیلم دوربین‌ها بسته به تعداد دوربین‌ها به مدت ۳۰ روز نگهداری شود.
- به جز مدیران و افراد تأییدی توسط آنها، هیچکس حق دیدن فیلم‌ها را ندارد.
- در صورت ضرورت مشاهده فیلم‌ها برای شخص موردنظر، باید مجوز مدیریت ارشد یا مدیر قسمت صادر شود.

۵-۱۲ -سرورها

- مدیریت و کنترل سرورها و کلیه تجهیزات مربوطه از حیث آماده‌به‌کاری سرویس‌های سازمان به‌منظور در دسترس قرار داشتن همیشگی شبکه و اطلاعات بر عهده واحد انفورماتیک است.

- تأمین به‌موقع قطعات یدکی مصرفی در سرورها مانند (هارد دیسک، پاور ماژول، رم و غیره...) انجام شود.
- سرورها به‌صورت دوره‌ای هر ۶ ماه یکبار برای جلوگیری از نشست گردوغبار و بروز آسیب به سرورها تمیز شوند.
- منبع برقی (UPS) مناسب و دوکاناله جهت جلوگیری از توقف ناگهانی سرورها، متناسب با توان مصرفی سرورها تأمین شود.
- بروزرسانی سخت‌افزار سرورها براساس نیازهای سازمانی به‌طور سه‌سالانه بررسی شود.
- نرم‌افزارهای سرورها جهت افزایش امنیت و بستن حفره‌های امنیتی به‌روزرسانی شوند.
- سرویس کلاسترینگ جهت راه‌اندازی خودکار سرور پشتیبان در مواقع بروز نقص فنی برای سرور اصلی سازمان، باید در هر زمان آماده به‌کار باشد.

۵-۱۳ -ارسال /دریافت اطلاعات از کارفرما/تأمین‌کنندگان

- استاندارد نحوه ارسال اطلاعات مشخص و به توافق طرفین برسد و بر اساس آن ارسال انجام شود.
- ارسال اطلاعات و انجام مکاتبات باید با مجوز مدیر واحد، با هدف کنترل دقیق انتقال اطلاعات از طریق مسئولین دفاتر و افراد مجاز، توسط مدیر هر واحد انجام شود.
- ارسال اطلاعات باید ترجیحاً در قالب فایل‌های بدون قابلیت ویرایش و از طریق رسانه‌های ذخیره‌سازی فقط خواندنی مانند CD ارسال شود.
- در هنگام دریافت اطلاعات، رسانه‌های ذخیره‌سازی قبل از ورود به چرخه اطلاعاتی سازمان، جهت جلوگیری از ورود برنامه مخرب، بررسی و پس از تأیید سلامت به‌کار گرفته شوند.
- استفاده از نرم‌افزارهای ارتباط جمعی مانند اینستاگرام، واتساپ و ... در سازمان ممنوع است.

۵-۱۴ -نگهداری و اداره اطلاعات محرمانه

- امنیت اطلاعات در زمان نگهداری و انتقال اطلاعات سازمان، در هر قالب و فرمت الکترونیکی، شامل تمامی بسترهای ذخیره‌سازی الکترونیکی، سیستم‌ها و نرم‌افزارهایی که توسط کارکنان، مدیران، تأمین‌کنندگان، کارکنان پاره‌وقت و موقتی و دیگر کارکنانی که مجاز به دسترسی به اطلاعات سازمان هستند، همچنین کاربران تأییدی که خارج از شبکه هستند، مورد استفاده قرار می‌گیرند، باید حفظ شود.
- اطلاعات نباید از طریق سیستم‌هایی که به سازمان تعلق ندارند، مورد استفاده قرار گیرند یا روی آنها ذخیره شوند، مگر اینکه مجوزهای خاص صادر شود.
- فکس اطلاعات تنها با مجوز مدیر واحد و از طریق مسئولین دفاتر انجام می‌شود.
- برای کاهش احتمال خطر افشا، از ارسال اطلاعات اضافی و غیرضروری خودداری شود.
- تأییدیه شماره فکس و فکس حتماً دریافت شود. (در صورت امکان جهت کاهش احتمال خطا از شماره‌گیر اتوماتیک استفاده شود).

- برای ارسال ایمیل‌های سازمانی نباید از آدرس‌های شخصی استفاده شود.
- ارسال ایمیل‌های سازمانی به خارج از شرکت تنها از طریق مسئولین دفاتر و افراد مجاز که توسط مدیر هر واحد مشخص شده‌اند، انجام شود.
- وقتی هر یک از کارکنان میز و محل کارشان را برای مدت زمانی ترک می‌کنند، تمامی اسناد حاوی اطلاعات محرمانه باید در محل‌های امن نظیر کشو یا کمدهای قفل‌دار نگهداری شوند. نباید هیچ‌گونه اطلاعات محرمانه‌ای در محل‌های باز و در دسترس در طول مدت عدم حضور، رها شوند.
- هرگونه گمان و حدس در مورد بروز نقص در امنیت و محرمانگی اطلاعات باید فوراً به مدیر واحد فناوری اطلاعات اطلاع‌رسانی شود.
- تأمین‌کنندگان خارج از سازمان باید به خاطر داشته باشند، ایشان نیز تحت همان قوانین امنیت اطلاعاتی هستند که کارکنان درون سازمان از آنها تبعیت می‌کنند.
- اطلاعات، بایگانی‌ها، فایل‌ها و نظایر آنها نباید در معرض دید بازدیدکنندگان باشد، مگر اینکه بازدیدکنندگان اختصاصاً مجاز به رویت اطلاعات باشند.
- اطلاعات در هر شکل و فرمتی باید در زمانی که دیگر مورد نیاز نیستند، به شیوه‌ای امن منهدم شوند.
- اطلاعات و دانشی که در مدت همکاری با سازمان به دست آمده است، پس از خاتمه همکاری باید به سازمان انتقال یابد. نقض محرمانگی احتمالی توسط افراد خاتمه همکاری، پیگیری شود و ممکن است منجر به اقدامات قانونی شود.

۵-۱۵ -سطوح دسترسی

- سطح دسترسی هر کاربر به اطلاعات با توجه به چارت سازمانی و مجوز مدیر واحد و دستور مدیر واحد انفورماتیک تعریف شود.
- فایل آماده توسط واحد انفورماتیک به مدیر واحد جهت مشخص کردن نام پوشه‌ها و اطلاعات موجود در آنها تحویل و مدیر واحد دسترسی کلیه کارشناسان خود را در آن ثبت و سپس توسط واحد انفورماتیک این دسترسی‌ها بر روی اطلاعات موجود در سرور تهیه می‌شود.
- تغییر هر کدام از سطوح دسترسی بدون مجوز مدیر واحد امکان‌پذیر نیست.
- مسئولیت حذف یا دستکاری اطلاعات که در عملکرد واحد یا سازمان اختلال ایجاد کند، در واحد مربوطه بر عهده کارشناسان و مدیر واحد می‌باشد.

۵-۱۶ -مدیریت حوادث امنیت اطلاعات

- حوادث امنیتی شامل (و نه محدود به) حملات ویروس‌ها، کرم‌ها، اسب‌های تروجان، استفاده غیرمجاز از دسترسی‌ها و تجهیزات نگهداری و پردازش اطلاعات و همچنین استفاده نادرست از آنها است.

- هنگام بروز حوادث امنیتی، مدیر واحد فناوری اطلاعات در جلسه‌ای با مدیر عامل ضمن تشریح ابعاد حادثه در خصوص تشکیل تیم مقابله با حوادث (متشکل از مدیر واحد انفورماتیک و مدیران درگیر) تصمیم می‌گیرند.
- مدیر واحد انفورماتیک، مدیریت و راهبری تیم مقابله با حوادث را بر عهده دارد.
- تیم مقابله با حوادث طبق "دستورالعمل مدیریت حوادث" اهداف ذیل را دنبال می‌کند:
  - الف- جلوگیری از حملات و دسترسی‌های غیرمجاز، علیه دارایی‌های اطلاعاتی سازمان.
  - ب- مهار خسارت‌های ناشی از ناامنی موجود در شبکه.
  - ج- کاهش رخنه پذیری به شبکه.
  - د- تأمین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت‌افزارها و نرم‌افزارها، متناسب با حساسیت آنها.
  - هـ- مدیریت فناوری اطلاعات باید در زمینه حوادث مختلف با دیگر سازمان‌های گروه در ارتباط باشد.
- تمامی فعالیت‌های مشکوک که شامل (و نه محدود به) حوادث امنیتی احتمالی می‌شوند، می‌بایست به مدیریت انفورماتیک سازمان گزارش شوند.

۵-۱۷ -دستگاه‌های قابل حمل و دورکاری

- ۵-۱۷-۱ -دستگاه‌های قابل حمل: این دستگاه‌ها شامل لپ‌تاپ، فلش، دوربین و موبایل و ... می‌باشد.
  - استفاده و انتقال دستگاه‌های قابل حمل با درخواست معاونت/مدیریت هر واحد و با مجوز صادره از واحد انفورماتیک امکان‌پذیر است.
  - بدون مجوز مدیریت انفورماتیک، ورود دستگاه به شرکت و اتصال به شبکه ممنوع است.
  - مسئولیت انتقال اطلاعات پس از مجوز به عهده معاونت/مدیریت و خود کاربر است.
  - اتصال موبایل یا تبلت به سیستم و شبکه سازمان ممنوع می‌باشد.
  - به‌کارگیری دستگاه‌های شخصی برای تبادل اطلاعات شرکت ممنوع است.
  - انتقال اطلاعات غیرضروری و اضافی با لپ‌تاپ‌ها برای شرکت در جلسات برون‌سازمانی اکیداً ممنوع است و اطلاعات موردنیاز همان جلسه یا مأموریت با درخواست مدیر قسمت بر روی لپ‌تاپ قرار گیرد.
- ۵-۱۷-۲ -دورکاری:
  - بستر دورکاری بر حسب نیاز و کسب مجوز مدیر مربوطه برای کارشناسان و مدیران به وجود می‌آید.
  - برای دسترسی به سیستم‌ها و منابع داخلی از راه دور، استفاده از **سیستم مدیریت دسترسی‌های ممتاز (PAM)** الزامی است. این سیستم کلیه اتصالات را واسطه‌گری، ضبط و کنترل می‌کند.

- در دورکاری، مجوز چک کردن ایمیل‌ها داده شده و تنظیمات آن را کارشناس واحد فناوری اطلاعات انجام می‌دهد.
- در صورت نیاز به دسترسی به اطلاعات درون سازمان، باید تمهیدات لازم اندیشیده و با درخواست مدیر واحد و مجوز مدیر ارشد سازمان انجام شود.
- کلیه تنظیمات مربوط روی دستگاه‌های انتقال داده شده در دورکاری توسط واحد انفورماتیک انجام شود.
- تحویل و برگرداندن سالم دستگاه‌ها از دورکاری بر عهده کاربر مربوطه است.
- تنظیمات شبکه و اطلاعات طوری توسط واحد انفورماتیک انجام شود که از راه دور نتوان به اطلاعات دسترسی پیدا کرد. برای اتصال به سیستم موردنظر کاربر تعریف و پس از انجام کار، دسترسی گرفته شود.

- ۵-۱۷-۳ -اتصال از راه دور به شبکه داخلی:
  - کارکنانی که مجوز دسترسی از راه دور دارند، موظف‌اند **صرفاً از طریق بستر امن PAM** به شبکه متصل شوند. استفاده از پروتکل‌های قدیمی یا نرم‌افزارهای دسترسی مستقیم مانندRRAS ، RDP یا AnyDesk **ممنوع** است.
  - کلیه افرادی که به‌وسیله **PAM**به شبکه سازمان دسترسی پیدا می‌کنند، باید به‌طور کامل از دارایی‌های اطلاعاتی سازمان محافظت کنند.
  - در خصوص موارد حساس مانند تعدیل یا اخراج نیرو، باید شرایط اتصال از جانب مدیر مربوطه اعلام و به تصویب مدیریت رسیده و دسترسی کاربر فوراً در **سیستم PAM** غیرفعال شود.
  - کلمات عبور تغییر یافته برای دسترسی‌های بعدی باید در اختیار واحد انفورماتیک قرار گیرد.

۵-۱۸ -نسخه پشتیبان(Backup)

- نسخه پشتیبان شامل نسخه پشتیبان بانک‌های اطلاعاتی و دیتای سازمان و نسخه پشتیبان از تمامی سیستم‌عامل‌های سرورها است. مسئول تهیه نسخ پشتیبان کارشناس واحد انفورماتیک با نظارت مدیر واحد است.
- کلیه اطلاعات سازمانی به‌صورت روزانه پشتیبان تهیه و این اطلاعات ۱ ماه بر روی سرور باقی بماند.
- سیستم‌عامل سرورها ۱۵ روز یک بار باید نسخه پشتیبان داشته باشند و محل ذخیره‌سازی آنها روی سرور است.
- در حال حاضر دیتای سرورها با نرم‌افزار **Synology**و سرورها با **Veeam Backup**نسخه پشتیبان تهیه شود.

- کلیه نسخ پشتیبان باید بر روی رسانه ذخیره‌سازی مورد تأیید و در خارج از محل و در یک مکان با تدابیر امنیتی مناسب نگهداری شوند.
- در هنگام تهیه نسخ پشتیبان باید تطابق با نسخه اصلی صورت گیرد و از صحت اطلاعات آن اطمینان حاصل شود.
- رسانه‌های تاریخ گذشته، باید نابود شوند. در بازه‌های زمانی مشخص، قابلیت بازیابی نسخ پشتیبان باید مورد آزمایش قرار گیرد تا از آن اطمینان حاصل شود.
- نسخ پشتیبان باید حاوی اطلاعات زیر باشد:
  - الف- نام سیستمی که از آن نسخه پشتیبان تهیه می‌شود.
  - ب- تاریخ تهیه نسخه پشتیبان.
  - ج- میزان اهمیت اطلاعاتی که از آنها نسخه پشتیبان گرفته شده است.
  - د- نام فردی که نسخه پشتیبان را تهیه کرده است.
  - هـ- تاریخ مصرف نسخه پشتیبان.
  - و- برای نسخه پشتیبان رمز تعریف گردد.
  - ز- خارج نمودن نسخ پشتیبان از سازمان به‌صورت ماهانه صورت گیرد.
  - ح- مسئولیت نگهداری از نسخ پشتیبان در خارج از سازمان تحت عنوان نسخ آرشیو بر عهده معاونت اداری/مالی است.
- به‌منظور برگرداندن اطلاعات از بین رفته، کلیه موارد ذکر شده در تهیه نسخه پشتیبان باید قابل بازیابی باشد.
- با مجوز مدیریت واحد و نیاز کاربر در صورت حذف اطلاعات از سرور با نرم‌افزار آکرونیس اطلاعات برگردانده شود.
- سیستم‌عامل‌های دارای مشکل نیز روی سرورها با نرم‌افزار **Veeam** برگردانده شود.
- اطلاعات بانک اطلاعاتی نیز که روی دیسک‌های بلوری ذخیره می‌شوند، با قابلیت خود نرم‌افزار SQL برگردانده شوند.

۱۹-۵ -امنیت فیزیکی و محیطی

- ۱-۱۹-۵ -دسترسی به تأسیسات اطلاعاتی: امنیت فیزیکی کلیه کامپیوترها و تجهیزات ارتباطی که متعلق به سازمان یا توسط سازمان مورد استفاده قرار می‌گیرند، باید توسط تمامی کارکنان، مدیران، تأمین‌کنندگان، کارکنان پاره‌وقت، کارکنان موقت، کارآموزان و دیگر کارکنانی را که مجاز به دسترسی به سیستم‌های اطلاعاتی سازمان شناخته‌اند، مورد توجه قرار گیرد.
  - دسترسی فیزیکی به محدوده‌های کنترلی (محدوده‌هایی که در آنها سیستم‌های اطلاعاتی یا اطلاعات حساس نگهداری می‌شوند، نظیر اتاق سرورها) می‌بایست مدیریت و ثبت شوند.

- تمامی محدوده‌های کنترلی می‌بایست نشانه‌گذاری و برچسب زده شوند و به تناسب حساسیت و اهمیت عملکردشان مورد حفاظت فیزیکی قرار گیرند.
- دسترسی به محدوده‌های کنترلی می‌بایست صرفاً برای کارکنان و تأمین‌کنندگان مجاز شناخته شود که مسئولیت کاریشان نیازمند دسترسی به محدوده مورد نظر است.
- درخواست برای دسترسی می‌بایست طبق روش اجرایی برقراری دسترسی صورت پذیرد.
- روش اجرایی دسترسی احتمالی برای محدوده‌های کنترلی می‌بایست آماده و در مواقع از کار افتادن سیستم کنترل خودکار دسترسی مورد استفاده قرار گیرد.
- کارت‌های دسترسی و یا کلیدها نمی‌بایست به‌صورت اشتراکی مورد استفاده قرار گیرند یا به دیگران قرض داده شوند.
- کارت‌های دسترسی یا کلیدهایی که دیگر مورد نیاز نیستند، می‌بایست به مسئول محدوده کنترلی برگردانده شوند. کارت‌ها نباید بدون طی مراحل بازگرداندن، به افراد دیگر اختصاص یابد.
- دسترسی بازدیدکنندگان به محدوده‌های کنترلی می‌بایست مطابق دستورالعمل بازدیدکنندگان باشد.

- ۵-۱۹-۲ -نواحی امن: جلوگیری از دسترسی فیزیکی غیرمجاز، خسارت و مداخله در اطلاعات و امکانات پردازش اطلاعات.
- ۵-۱۹-۳ -حصار امنیتی فیزیکی:
  - وجود یک اتاق برای نگهداری سرورها و رک‌ها الزامی است.
  - کنترل دمای اتاق در دمای **۲۰ درجه سانتی‌گراد** نگه داشته شود.
  - آن دسته از تجهیزاتی که در سطح سازمان به دلایل ساختار فیزیکی نصب هستند، در رک مجهز به قفل نگهداری شوند.
- ۵-۱۹-۴ -کنترل‌های مداخل فیزیکی: کلیه مداخل فیزیکی باید مجهز به قفل و دوربین‌های مداربسته باشد.
- ۵-۱۹-۵ -امن‌سازی دفاتر، اتاق‌ها و امکانات: باید محل‌های سرورها ایزوله و به جز مسئولین واحد فناوری اطلاعات کسی اجازه دسترسی به سرورها و سوئیچ‌ها و تجهیزات را نداشته باشد.
- ۵-۱۹-۶ -محافظت در مورد تهدیدهای محیطی و بیرونی:
  - انواع تهدیدهای متعارف مصادیق محیطی (E) مانند زلزله، گردباد، رعد و برق، سیل، نوسان برق، دما و رطوبت زیاد، گرد و غبار، تخریب محیط ذخیره‌سازی.
  - مصادیق اقدام انسان- تصادفی (A) مانند نقص در سیستم تهویه، نقص در سخت‌افزار، اشکال در تعمیرات، اشکال در نرم‌افزار، استفاده از نرم‌افزار توسط افراد غیرمجاز، استفاده از نرم‌افزار به شیوه‌ای

غیرمجاز، استفاده از نرم‌افزار خارج از قواعد، نقص فنی در اجزای شبکه، خطا در انتقال، آسیب دیدن خطوط، ترافیک بیش از اندازه در شبکه، حذف فایل، نقض در خدمات ارتباطی.

- مصادیق عمدی (D) مانند اقدامات صنعتی، حمله با بمب، استفاده از سلاح، آتش‌افروزی، آسیب عمدی، دزدی، استفاده غیرمجاز از محیط ذخیره‌سازی، تغییر هویت و جعل هویت، نرم‌افزارهای مخرب، استفاده نادرست از دسترسی متعارف، دسترسی غیرمجاز به شبکه، استفاده غیرمجاز از تجهیزات شبکه، شنود، نفوذ در تجهیزات ارتباطی، تحلیل ترافیک شبکه، تغییر مسیر پیام، انکار و سرباز زدن، استفاده نادرست از منابع.
- کلیه سرورها و یو پی اس‌ها و آنتن‌ها با تهدیدهای موجود در جدول باید کنترل شوند. این مسئولیت بر عهده واحد انفورماتیک می‌باشد.

- ۵-۱۹-۷ -امنیت کابل‌کشی: کلیه کابل‌کشی‌ها باید چک و اگر آسیب یا نقصی در کابل‌کشی هست باید توسط واحد انفورماتیک تعمیر شود. این کابل‌کشی شامل کابل‌کشی شبکه و تلفن می‌باشد.
- ۵-۱۹-۸ -خروج دارایی‌ها: تجهیزات، نرم‌افزارها و اطلاعات بدون مجوز قبلی نباید از شرکت خارج شوند. این مجوز بر عهده واحد انفورماتیک و انبار با هماهنگی مدیر مربوطه است.
- ۵-۱۹-۹ -امنیت تجهیزات و دارایی‌های خارج از محوطه: امنیت تمام دارایی‌های درون پروژه‌ها بر عهده مدیر پروژه می‌باشد.
- ۵-۱۹-۱۰ -امحا یا استفاده مجدد از تجهیزات به‌صورت امن:
  - نرم‌افزارهای زیادی وجود دارند که می‌توانند برای بازیابی فایل‌ها و اطلاعات حذف شده از روی تجهیزات سخت‌افزاری (فرمت شده) مورد استفاده قرار گیرند. برای کاهش احتمال خطر انتشار بدون مجوز اطلاعات حساس و محرمانه، می‌بایست اطلاعات موجود بر روی تجهیزاتی که پیشتر مورد استفاده قرار گرفته‌اند، به‌طور امن حذف شوند. پس از این عملیات، بازیابی اطلاعات توسط نرم‌افزارهای معمولی امکان‌پذیر نخواهد بود و برای بازیابی می‌بایست تکنیک‌های تخصصی به‌کار گرفته شوند. همچنین برای حذف اطلاعات می‌توان از روش‌هایی استفاده نمود که بازیابی توسط تکنیک‌های تخصصی نیز امکان‌پذیر نباشد.
  - تمامی اطلاعات سیستم‌های کامپیوتری و رسانه‌های مرتبط با آنها که ممکن است حاوی اطلاعات حساس یا محرمانه باشند، می‌بایست پیش از استفاده مجدد یا انهدام، پاک شوند.
  - اطلاعات تمامی بسترهای ذخیره‌سازی اطلاعات سیستم‌ها و قطعاتی که در سازمان مجدداً مورد استفاده قرار می‌گیرند، باید با یک نرم‌افزار مورد تأیید پاک شوند. در برخی از موارد باید از سیستم‌ها پیش از استفاده مجدد یک نسخه پشتیبان کامل تهیه شود.

- تمامی بسترهای ذخیره‌سازی سیستم‌ها و تجهیزاتی که مورد استفاده مجدد قرار گرفته، فروخته، یا بخشیده می‌شوند، یا حتی به‌عنوان وسایل غیرقابل استفاده به بیرون از سازمان منتقل می‌شوند، لازم است توسط نرم‌افزار مورد تأیید پاک شوند.
- تمامی عملیات پاک کردن یا انهدام تجهیزات می‌باید با اطلاعات زیر ثبت شوند: تاریخ و زمان عملیات، نام، عنوان و امضای کارشناس مربوطه، شرح اقدامات انجام گرفته.

• ۵-۱۹-۱۱ -میز پاک و صفحه پاک: برقراری استانداردهای امنیت فیزیکی ایستگاه‌های کاری و برای پیشگیری از سرقت ایستگاه‌های کاری تمامی کارکنان را که مجاز به دسترسی به سیستم‌های اطلاعاتی سازمان شناخته‌اند، ضروری است.

- کاربران ایستگاه‌های کاری نباید هیچ دستگاه جانبی که فاقد تأییدیه واحد انفورماتیک است را به ایستگاه‌های کاری متصل کنند.
- مانیتورهای ایستگاه‌های کاری می‌بایست به‌گونه‌ای قرار گیرند که از دیده شدن اطلاعات حساس توسط افراد غیرمجاز جلوگیری شود.

۵-۲۰ -امنیت سیستم تلفنی ویپ

در راستای حفظ محرمانگی و جلوگیری از شنود، دستکاری و سوءاستفاده از سیستم تلفنی سازمان، موارد زیر رعایت گردد:

- راه‌اندازی سیستم VoIP فقط توسط واحد فناوری اطلاعات و روی زیرساخت امن صورت گیرد.
- تمامی ارتباطات VoIP باید از طریق VPN داخلی یا VLAN مجزا منتقل شوند.
- استفاده از SIP-TLS و SRTP برای رمزگذاری سیگنالینگ و مکالمات الزامی است.
- دسترسی به پنل مدیریت مرکز تلفن (PBX/IPPBX) فقط برای مدیر IT مجاز است.
- اتصال دستگاه‌های Softphone صرفاً با نام کاربری سازمانی و رمز قوی مجاز است.
- ایجاد، حذف و تغییر تنظیمات داخلی‌ها (Extension) فقط با درخواست کتبی مدیر واحد انجام شود.
- تمامی لاگ‌های تماس و گزارش تلاش‌های ناموفق باید روزانه توسط مدیر IT پایش شوند.
- اتصال VoIP از خارج سازمان بدون VPN ممنوع است.
- هرگونه تلاش برای شنود، دستکاری بسته‌ها، Brute Forceیا ثبت تماس غیرمجاز به‌عنوان حادثه امنیتی ثبت و پیگیری می‌شود.

۵-۲۱ -ممنوعیت خروج اطلاعات از سازمان

با توجه به نیاز سازمان برای حفاظت از اطلاعات محرمانه و جلوگیری از سرقت یا نشت داده:

- خروج اطلاعات در هر قالبی (فیزیکی یا دیجیتال) تنها با مجوز کتبی مدیریت و ثبت در سیستم خروج دارایی امکان‌پذیر است.

- ذخیره‌سازی اطلاعات سازمان روی فلش، هارد اکسترنال، CD/DVD، موبایل و لپ‌تاپ شخصی ممنوع است.
- ارسال فایل از طریق ایمیل شخصی، پیام‌رسان‌ها، شبکه‌های اجتماعی، وب‌سرویس‌های ذخیره‌سازی (Google Drive)، Dropbox و (... ممنوع است.
- هرگونه عکس‌برداری یا فیلم‌برداری از صفحه‌نمایش، مانیتور یا سیستم‌ها بدون مجوز مدیریت ممنوع است.
- فایل‌های حساس فقط باید روی سرور داخلی و با سطح دسترسی کنترل‌شده نگهداری شوند.
- چاپ اطلاعات حساس فقط با تأیید مدیر واحد و ثبت در فرم مخصوص مجاز است.
- نشت اطلاعات حتی سهوی، مطابق قوانین داخلی و مقررات ملی، پیگیری قانونی خواهد داشت.

۲۲-۵ -بازدید دوره‌ای اتاق سرور، برق، کولینگ و سنسورها

در راستای افزایش پایداری عملیاتی و کاهش ریسک‌های محیطی:

- واحد IT موظف است حداقل ماهانه یک‌بار بازدید کامل اتاق سرور را انجام دهد.
- موارد زیر باید در چک‌لیست بازدید ثبت و نگهداری شود:
  - **الف) سیستم برق**
    - عملکرد صحیح UPS ، برق ورودی، تثبیت‌کننده‌ها و باتری‌ها
    - تست هشدار قطع برق
    - بررسی میزان بار مصرفی سرورها و UPS
  - **ب) سیستم سرمایش(Cooling)**
    - بررسی عملکرد کولرهای اختصاصی اتاق سرور
    - حفظ دمای بین ۲۰ تا ۲۳ درجه
    - پایش پیوسته رطوبت محیط
    - ثبت دمای روزانه در فرم لاگ اتاق سرور
  - **ج) سنسورها و تجهیزات نظارتی**
    - سنسور حرارت
    - سنسور دود(Fire Detection)
    - سنسور نشت آب
    - سنسور ولتاژ و ارت
    - سیستم اعلام و اطفای حریق
  - **د) ساختار فیزیکی**
    - بررسی رک‌ها، قفل‌بودن درب‌ها و وضعیت کابل‌کشی

- کنترل دسترسی فیزیکی بر اساس کارت/اثر انگشت
- بازبینی دوربین مداربسته اتاق سرور

- تمامی موارد بالا باید در سامانه نگهداری رکوردها ثبت و نزد مدیر IT بایگانی شود.

۲۳-۵ -نگهداری از شبکه یکپارچه مبتنی بر VPN داخلی

برای افزایش امنیت ارتباطات بین واحدها، پروژه‌ها و دفاتر مختلف سازمان:

- تمامی ارتباطات بین نقاط مختلف سازمان باید از طریق VPN داخلی امن (Site-to-Site یا Client-to-Site) برقرار شود.
- پروتکل‌های مجاز شامل OpenVPN ، L2TP/IPSec یا SSL-VPN با رمزنگاری قوی هستند.
- هرگونه دسترسی ریموت بدون VPN رسمی سازمان ممنوع است.
- کلیه تونل‌های VPN باید دارای موارد زیر باشند:
  - احراز هویت دو مرحله‌ای(2FA)
  - گواهی دیجیتال معتبر(Certificate-Based Authentication)
  - رمزگذاری AES-256
- دسترسی VPN برای کاربران موقت باید زمان‌دار و محدود باشد.
- لاگ اتصال و قطع اتصال کاربران VPN باید ثبت و ماهانه بررسی شود.
- هر پروژه یا بخش جدید، تنها از طریق VLAN جداگانه یا کانال VPN اختصاصی به شبکه متصل می‌شود.
- تمام ترافیک VPN باید از فایروال مرکزی عبور کند و تحت پایش قرار گیرد.