

منشور سازمانی رویه های اجرایی

"حفظ محرمانگی اطلاعات نهانی و داده های الکترونیکی"

شرکت گسترش صنایع روی ایرانیان (سهامی عام)

تصویب کننده	تهیه کننده	
مدیر عامل	مدیر واحد فناوری اطلاعات IT	سمت
مهندس سید فلاح حسین زاده نودهی	مهندس سعید علیمی	نام و نام خانوادگی
		امضاء



تذکره:

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.

۱- اهداف

این روش اجرایی با هدف حفظ امنیت و صحت اطلاعات، استفاده صحیح از امکانات سخت افزاری و نرم افزاری و همچنین حصول اطمینان از پایداری شبکه از لحاظ ارتباطات، تهیه و تدوین گردیده است. امنیت اطلاعات: شامل محرمانگی، حفظ صحت و یکپارچگی، و دسترس پذیری در زمان ایجاد، انتقال و نگهداری است.

۲- دامنه کاربرد

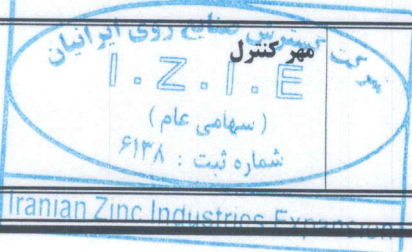
این روش اجرایی شامل کلیه اطلاعات سازمان (اعم از اطلاعات داخل شرکت و اطلاعات مربوط به کارفرمایان)، سیستم های کامپیوتری و تجهیزاتی است که به شبکه متصل و درون سازمان قرار دارند. همچنین، سیستم هایی که با نام سازمان در خارج از شرکت (مانند پروژه ها) و کلیه کاربران داخلی و خارجی شبکه که با سیستم های سازمان درگیر هستند را نیز در بر می گیرد.

۳- تعاریف

- اطلاعات: داده های پردازش شده که شامل تمامی اطلاعات دیجیتالی مبنایی برای تصمیم گیری می باشند. اطلاعات یک دارایی است که همانند سایر دارایی ها باید حفظ و نگهداری شود.
- اطلاعات شامل: متون، نقشه ها، تصاویر، نامه ها، پرونده ها، اسناد، فایل های کامپیوتری، اطلاعات توصیفی و جغرافیایی و ...، چه در داخل شبکه و سرورها و چه بر روی کلاینت ها و کامپیوترهای مستقل. همچنین مستندات الکترونیکی، مراسلات متداول، رسانه های الکترونیکی، سوابق پایگاه داده، ایمیل ها، نوارها، DVD ها، CD ها، فیلم ها و اطلاعات بیان شده در جلسات.
- کاربران: شامل کارکنان، پیمانکاران مرتبط با شبکه و سایر کاربرانی که به نحوی با بخش های مدیریتی یا کاربردی درون سازمانی شبکه در ارتباط می باشند.
- نرم افزار: شامل سیستم عامل ها مانند Windows، Linux، نرم افزارهای کاربردی عمومی (مانند Office، نرم افزارهای کاربردی سازمانی (مانند سیستم اتوماسیون اداری)، نرم افزارهای کاربردی اختصاصی

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.



- (مانند سیستم های فنی و مهندسی)، نرم افزارهای مدیریت شبکه و سیستم های تحت وب (مانند File Server, My SQL, SQL Server, Email Server, Active Directory, ...).
- **سخت افزار:** شامل ایستگاه های کاری، سرویس دهنده ها، Data Projector ها، PC ها، Laptop ها، تجهیزات شبکه و انتقال داده (مانند Router ها، Switch ها، Hub ها)، چاپگرها، پوشگرها، و تجهیزات سیار انتقال اطلاعات (مانند Flash Memory ها، CD ها، DVD ها، دوربین های دیجیتالی و ...).
 - **ارتباطات:** شامل کابل های فیبرنوری، CAT6 و CAT7، ارتباطات شبکه سازمان با سایر شبکه های 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 گردیده اند و دارای نام کاربری در دامنه سازمان می باشند.
 - **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 سازمان های بیرونی به سازمان سرویس می دهند.
 - **سیستم: PAM (Privileged Access Management)** سیستم مدیریت دسترسی های ممتاز، ابزاری که برای کنترل، پایش و ضبط کلیه جلسات دسترسی کاربران ممتاز به منابع حساس شبکه (مانند سرورها، تجهیزات شبکه و دیتابیس ها) استفاده می شود.
 - **پورتال سازمانی:** هرگونه سامانه یا نرم افزار تحت وب که برای تسهیل امور داخلی سازمان (مانند اتوماسیون اداری، پورتال منابع انسانی، Intranet، مدیریت پروژه ها (طراحی شده و صرفاً توسط کارکنان یا کاربران مجاز داخلی مورد استفاده قرار می گیرد).

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، به روزآوری، نظارت بر حسن 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 زیرساخت های پورتال ها را دارا است.
- **معاونین و مدیران واحدها:** مسئول نظارت بر حسن اجرای روش اجرایی در واحد تحت مدیریت خود هستند.
- **مدیران پروژه ها:** مسئول اجرای روش اجرایی در تمام مقاطع اجرای پروژه ای که مدیریت آن را بر عهده دارند، و در تمام واحدهای درگیر هستند.

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 منابع روی ایرانیان
I.Z.I.E
(سهامی عام)
شماره ثبت: ۶۱۳۸

- **کاربران:** مسئول اجرای روش اجرایی هستند.
- **مدیر سیستم ها و روش ها:** مسئول پایش روش اجرایی و گزارش آن به مدیر عامل در مقاطع مقتضی است.
- **مشاور انفورماتیک:** مسئول همکاری با مدیر واحد فناوری اطلاعات در پیاده سازی و انتخاب سخت افزار و نرم افزار 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 رویه های اجرایی

- اطلاعات سازمان صرفاً توسط افراد مجاز قابل دسترسی باشند.
- محرمانگی اطلاعات می بایست همواره در کل شرکت، در پروژه ها و بین واحدهای سازمانی حفظ شود.
- در کلیه فرایندهای امنیتی، یکپارچگی اطلاعات حفظ گردد.
- پیاده سازی سیاست های امنیتی نباید اختلالی در روند کاری سازمان و واحدها ایجاد کند.
- آموزش های لازم در مورد امنیت اطلاعات و سیاست های امنیتی مربوط به کل سازمان است.
- تمامی رخنه های امنیت اطلاعات و ضعف های احتمالی باید توسط همه کاربران گزارش شده و به آنها رسیدگی گردد.
- تبادل اطلاعات بین سازمانی همواره باید از طریق کانال های مجاز و مورد تأیید سازمان صورت گیرد.
- تمام دستورالعمل های امنیتی مصوب برای کلیه سازمان یکسان است و موارد استثنا، تنها در صورت دستور کتبی مدیریت ارشد اعمال می شود.
- هرگونه خارج نمودن و انتشار اطلاعات شرکت، مگر با اخذ مجوز از مقامات ذیصلاح، تخلف محسوب می شود.
- کلیه نرم افزارهای داخلی که از طریق آنها تولید محتوا می شود، باید مشخص، استانداردسازی و منطبق بر سیاست های امنیتی سازمان به کار 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 می شود.
- 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 کلاینت ها، سرورها و دیتابیس ها، که جزء دسترسی مجاز یک کاربر نمی باشد، با هرگونه ابزار سخت افزاری یا نرم افزاری، تخلف محسوب می شود.
- در راستای اجرای دقیق این روش اجرایی، موارد به شرح زیر طبقه بندی می گردد:

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.



۵-۱- پست الکترونیکی

- ۵-۱-۱- ایمیل های سازمانی: معرفی و ایجاد ایمیل های سازمانی توسط کارشناسان IT با نظر مدیران هر واحد انجام می شود.
- ۵-۱-۲- ایمیل های شخصی: استفاده متعارف از منابع سازمان برای ایمیل های شخصی پذیرفتنی است، ولی ایمیل های غیرمرتبط با کار می بایست در پوشه جداگانه و مجزا از ایمیل های کاری نگهداری شوند. در ضمن ایمیل های شخصی باید از ایمیل های سازمانی جدا شوند.
- کارکنان سازمان نباید انتظار داشته باشند پیام هایی که در سیستم پست الکترونیکی سازمان ذخیره، ارسال و دریافت می کنند، در قالب حیطه شخصی آنها تلقی و محرمانه باشد. سازمان ممکن است بدون هشدار قبلی به نظارت و بررسی ایمیل ها بپردازد.
- فایل نگهداری ایمیل های سازمانی تنها در دسترس خود کاربر و کارشناس IT می باشد.
- تمامی ایمیل هایی که حاوی اطلاعات سازمانی هستند، به طور روزانه نسخه پشتیبان تهیه و در سرور نگهداری شوند.
- ارسال ایمیل سازمانی برای خارج از شرکت (اعم از کارفرمایان، تأمین کنندگان و سایر اشخاص حقیقی) تنها توسط مدیران و پست های 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 می شود. اطلاعات فردی در **درايو** هر سیستم قابل مشاهده است.

- کاربران از قرار دادن اطلاعات سازمانی در **درايو** خودداری کنند.
- اطلاعاتی که کاملاً شخصی است، نباید در سیستم نگهداری شود.
- مسئولیت پاک شدن اطلاعات فردی بر عهده کاربر است.
- قرار دادن فایل های Multi Media و عکس در **درايو** امکان پذیر نمی باشد.
- مدیران هر واحد باید دسته بندی منظم و دقیقی را برای حفظ و نگهداری اطلاعات به منظور دسترسی سریع ایجاد کنند و کلیه کاربران موظف به رعایت آن هستند.
- کلیه فایل های مهم باید رمز عبور داشته باشند.

۵-۳- نرم افزار ERP

تذکره:

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
I.Z.I.E
(سهامی عام)
شماره ثبت: ۶۱۳۸

- نرم افزار ERP شامل سیستم های مالی، منابع انسانی، انبار، حقوق و دستمزد، اموال و ... دارای زیرسیستم های مختلفی است. کاربر هر واحد با توجه به مجوز صادره از طریق معاونت اداری و مالی به آن دسترسی دارد.
- این نرم افزار دارای سطوح دسترسی مختلفی است. مسئولیت اجرای مجوز به عهده مدیر واحد فناوری اطلاعات است.
- کلیه اطلاعات این نرم افزار بر روی سرور نگهداری شود.
- در صورت لزوم، تبادل اطلاعات (رپلیکیشن بین سرورها) بین سرورهای دفتر مرکزی جهت به روزرسانی اطلاعات مربوط به سیستم ERP و پروژه های سازمان انجام شود.
- هر کاربر با نام کاربری و رمز عبور خود وارد سیستم می شود 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 به منظور برقراری درست ارتباط به طور مستمر باید کنترل و چک شود.
- دستورات پینگ برای ارتباط با روتر دفتر مرکزی و پروژه ها و شرکت های مشارکت کننده باید کنترل شود.
- در صورت قطع شدن ارتباط، تمامی آدرس های IP ارتباط بین دو نقطه کنترل می شود.

۵-۴- اطلاعات مربوط به Active Directory

- تعریف/حذف کاربران و رمزهای کاربران، اطلاعات مربوط به پروفایل های آنها، ایجاد دسترسی ها و مدیریت سرور DNS، DHCP بر 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 سریع ترین 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 ۱۰ حرف 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 qwert 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 نمی تواند برای حداقل ۳ دوره قبل استفاده گردد.
- ۵-۴-۲- ایجاد و مدیریت دسترسی کاربران:
 - کلیه دسترسی ها به اطلاعات مرتبط با حوزه کاری کاربر باید با درخواست مستند پس از تأیید توسط مدیر مستقیم ایجاد شوند.

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.



Iranian Zinc Industries Expansion

- کلیه دسترسی ها 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 درخواست های تأیید شده توسط مدیر عامل، لازم الاجرا هستند.
- کلیه کاربران سازمان باید بخشنامه قوانین امنیت اطلاعات سازمان را مطالعه و امضاء کرده باشند.
- کلیه اسامی کاربری در سیستم می بایست به صورت منحصر به فرد ایجاد شوند.
- کاربرانی که بیش از ۱۰ روز از کد کاربری خود استفاده نکنند، غیرفعال می شوند.
- مراحل ایجاد و تغییر کاربران باید مستند شود و در دوره های 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.

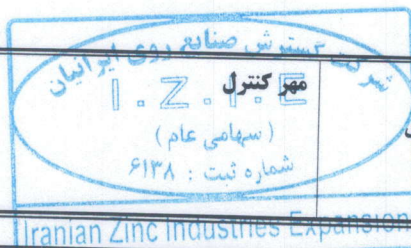
۵-۵- مدیریت محتوا، طراحی و انتشار وبسایت

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

- مالکیت و مسئولیت محتوا: کلیه محتوا و داده های منتشر شده در وبسایت سازمان (شامل متن، تصاویر، طراحی، کد) دارای سازمان محسوب می شود. مسئولیت تأیید صحت، به روز بودن و انطباق قانونی محتوای منتشر شده مستقیماً بر عهده مدیر توسعه بازار/واحد محتوا است.
- استانداردهای طراحی و برندینگ: تمامی طرح ها و قالب های 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) پیاده سازی، تست و تأیید شوند.
- کیفیت و SEO: محتوا باید با هدف افزایش اعتبار سازمانی، رعایت اصول فنی سئو و بهبود رتبه بندی در موتورهای جستجو تولید و به طور مستمر پایش شود.

۵-۶- امنیت زیرساخت وب، دامنه و هاستینگ

به منظور محافظت از زیرساخت های اینترنتی سازمان در برابر حملات و دسترسی های غیرمجاز:



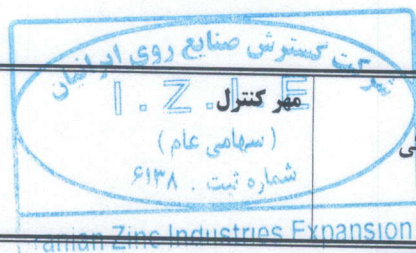
تذکره:

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.

- مدیریت زیرساخت: مدیریت ثبت، تمدید دامنه، تنظیمات DNS و کنترل پنل هاستینگ (شامل دسترسی به پایگاه داده و فایل ها) صرفاً بر عهده واحد فناوری اطلاعات و ارتباطات است.
- رمزنگاری ترافیک: (HTTPS) استفاده از گواهی های معتبر SSL/TLS و رمزنگاری تمامی ترافیک ورودی و خروجی وبسایت (HTTPS) الزامی است.
- حفاظت و به روزرسانی پلتفرم: به روزرسانی های امنیتی سیستم مدیریت محتوا (CMS)، افزونه ها (Plugins)، کتابخانه ها و سیستم عامل سرور میزبان باید به طور منظم و فوری توسط واحد IT انجام پذیرد.
- فایروال نرم افزار وب: (WAF) جهت جلوگیری از حملات متداول وب (مانند SQL Injection و XSS)، نصب و فعال سازی یک فایروال نرم افزار وب (WAF) یا ابزار امنیتی معادل در لایه دسترسی الزامی است.
- دسترسی های ممتاز: دسترسی به پنل های مدیریتی سطح بالا (مانند SSH, Plesk/FTP/Database) باید با رمزهای بسیار قوی، احراز هویت دوحلای (2FA) و محدود به آدرس های IP مجاز سازمان باشد.

۷-۵- نگهداری و امنیت پورتال های سازمانی

- این دستورالعمل برای حفظ امنیت سامانه ها و نرم افزارهای تحت وب داخلی (Intranet)، پورتال HR، سیستم مدیریت پروژه ها، امور سهام، تدارکات و (... اعمال می شود):
- جداسازی شبکه: پورتال های سازمانی باید به لحاظ فیزیکی یا منطقی (با استفاده از VLAN) از شبکه عمومی و وبسایت رسمی سازمان جدا شوند و دسترسی به آن ها فقط از طریق شبکه داخلی سازمان یا بستر VPN/PAM مجاز است.
 - احراز هویت کاربران: احراز هویت کاربران پورتال ها 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 دوحلای الزامی است.
 - کنترل دسترسی مبتنی بر نقش: (RBAC) سطوح دسترسی کاربران به پورتال ها باید کاملاً مبتنی بر نقش های سازمانی آن ها بوده و با تأیید مدیر واحد مربوطه تنظیم شود.
 - بروزرسانی و تست آسیب پذیری: به روزرسانی منظم سیستم عامل، دیتابیس و کدهای پورتال های سازمانی توسط واحد IT انجام شود. تست های دوره ای ارزیابی آسیب پذیری (Vulnerability Assessment) و نفوذپذیری (Penetration Testing) باید بر روی این سامانه ها اجرا شود.
 - پایش لاگ: کلیه لاگ های دسترسی، خطاها و فعالیت های مدیران سیستم در پورتال ها باید به طور مستمر پایش و برای مدت حداقل ۶ ماه نگهداری شوند.



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.

تذکر:

Zamin Zinc Industries Expansion

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

- این نرم افزار جهت ثبت ورود و خروج کاربران استفاده می شود. واحد اداری مسئولیت استفاده از این نرم افزار 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 دسترسی های 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 می کند.
- استفاده از اینترنت برای انجام کار شخصی ممنوع است.
- نصب و به کارگیری نرم افزارهایی که به اینترنت نیاز دارند باید با مجوز مدیریت هر دپارتمان انجام شود.
- میزان استفاده کاربران از اینترنت به طور ماهانه به مدیریت ارشد گزارش شود.
- هر کاربر تنها با نام کاربری و کلمه عبور خود می تواند 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 نمی باشند، مگر با تشخیص مدیریت واحد و به صورت محدود در زمان معین (این زمان بیشتر از مدت یک روز کاری نمی تواند باشد).
- کاربران مجاز به استفاده از اینترنت وایرلس حق انتقال رمز را به سایر کارکنان ندارند.
- در صورت به کارگیری اینترنت وایرلس، با توجه به محرمانگی اطلاعات، ورود به شبکه تحت هیچ شرایطی امکان پذیر نمی باشد.

۵-۱۰- حفاظت در برابر ویروس ها و باج افزارها

- این بخش کلیه افرادی را که از منابع اطلاعاتی سازمان استفاده می کنند، در بر می گیرد.
- به منظور جلوگیری از ورود و همچنین شناسایی و مقابله با ویروس ها، کرم ها و اسب های تروجان و ... از نرم افزار Kaspersky استفاده می شود. این نرم افزار روزانه از اینترنت به روزرسانی خواهد شد.



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.

- کلیه کامپیوترهایی که به سازمان تعلق دارند یا توسط سازمان مدیریت می شوند، همین طور لپ تاپ هایی که به شبکه سازمان متصل می شوند یا به صورت مستقل مورد استفاده قرار می گیرند، می بایست از نرم افزار آنتی ویروس و تنظیمات مورد تأیید واحد فناوری اطلاعات سازمان استفاده کنند.
- تمامی کامپیوترهایی که به سازمان تعلق ندارند یا تحت مدیریت سازمان نمی باشند، پیش از هرگونه ارتباط و اتصال به منابع اطلاعاتی سازمان، باید از نرم افزار ضد ویروس و تنظیمات مورد تأیید مدیر واحد فناوری اطلاعات سازمان استفاده کنند.
- نرم افزار ضد ویروس نباید غیرفعال (Disable) شود. دسترسی کاربران به این گزینه امکان پذیر نیست.
- تنظیمات نرم افزار ضد ویروس نباید به گونه ای تغییر کند که قابلیت تأثیرگذاری آن را کاهش دهد.
- تنظیمات به روزرسانی نرم افزار ضد ویروس نباید به گونه ای تغییر کند که بازه های زمانی به روزرسانی آن را کاهش دهد.
- هر سرویس دهنده ای که به شبکه سازمان متصل است، باید از نرم افزار ضد ویروس مورد تأیید سازمان استفاده کند.
- تمام گذرگاه های پست الکترونیکی باید از نرم افزار ضد ویروس مورد تأیید سازمان استفاده کنند و تمامی نامه های ورودی و خروجی می باید توسط این نرم افزار کنترل شوند.
- هر ویروسی که به صورت خودکار توسط نرم افزار پاک نشود، باید در اولین زمان ممکن به واحد فناوری اطلاعات گزارش شود.
- کارشناس واحد فناوری اطلاعات باید به روزرسانی آنتی ویروس را چک کند و در صورت مشکل باید با شرکت موردنظر تماس برقرار کند.

۵-۱۱- اطلاعات دوربین ها

- مدیریت و کنترل دوربین ها و کلیه اطلاعات مربوط به نرم افزار دوربین ها (شامل نام کاربری، کلمه عبور، نرم افزار نصب) و همچنین معرفی کاربرانی که مجاز به دیدن فیلم ها هستند، با واحد فناوری اطلاعات است.
- نرم افزار دوربین ها حتماً باید در سرور و نسخه کلاینت آن در کامپیوترهای کاربران مجاز نصب شود.
- فیلم ضبط شده دوربین ها باید در سرور نگهداری شود و این اطلاعات ذخیره شده باید چک شود.
- فیلم دوربین ها بسته به تعداد دوربین ها به مدت ۳۰ روز نگهداری شود.
- به جز مدیران و افراد تأییدی توسط آنها، هیچکس حق دیدن فیلم ها را ندارد.
- در صورت ضرورت مشاهده فیلم ها 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 آماده به کاری سرویس های سازمان به منظور در دسترس قرار داشتن همیشگی شبکه و اطلاعات بر عهده واحد انفورماتیک است.

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.



- تأمین به موقع قطعات یدکی مصرفی در سرورها مانند (هارد دیسک، پاور ماژول، رم و غیره...) انجام شود.
- سرورها به صورت دوره ای 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 سخت افزار سرورها براساس نیازهای سازمانی به طور سه سالانه بررسی شود.
- نرم افزارهای سرورها جهت افزایش امنیت و بستن حفره های امنیتی به روزرسانی شوند.
- سرویس کلاسترینگ جهت راه اندازی خودکار سرور پشتیبان در مواقع بروز نقص فنی برای سرور اصلی سازمان، باید در هر زمان آماده به کار باشد.

۱۳-۵- ارسال / دریافت اطلاعات از کارفرما / تأمین کنندگان

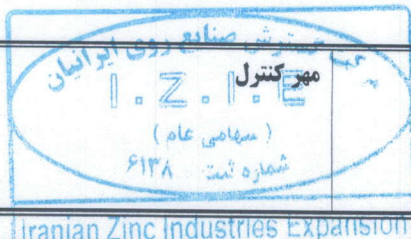
- استاندارد نحوه ارسال اطلاعات مشخص و به توافق طرفین برسد و بر اساس آن ارسال انجام شود.
- ارسال اطلاعات و انجام مکاتبات باید با مجوز مدیر واحد، با هدف کنترل دقیق انتقال اطلاعات از طریق مسئولین دفاتر و افراد مجاز، توسط مدیر هر واحد انجام شود.
- ارسال اطلاعات باید ترجیحاً در قالب فایل های بدون قابلیت ویرایش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

۱۴-۵- نگهداری و اداره اطلاعات محرمانه

- امنیت اطلاعات در زمان نگهداری و انتقال اطلاعات سازمان، در هر قالب و فرمت الکترونیکی، شامل تمامی بسترهای ذخیره سازی الکترونیکی، سیستم ها و نرم افزارهایی که توسط کارکنان، مدیران، تأمین کنندگان، کارکنان پاره وقت و موقتی و دیگر کارکنانی که مجاز به دسترسی به اطلاعات سازمان هستند، همچنین کاربران تأییدی که خارج از شبکه هستند، مورد استفاده قرار می گیرند، باید حفظ شود.
- اطلاعات نباید از طریق سیستم هایی 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 می شود.
- 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 شماره گیر اتوماتیک استفاده شود).

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.



Iranian Zinc Industries Expansion

- برای ارسال ایمیل های سازمانی نباید از آدرس های شخصی استفاده شود.
- ارسال ایمیل های سازمانی به خارج از شرکت تنها از طریق مسئولین دفاتر و افراد مجاز که توسط مدیر هر واحد مشخص شده اند، انجام شود.
- وقتی هر یک از کارکنان میز و محل کارشان را برای مدت زمانی ترک می کنند، تمامی اسناد حاوی اطلاعات محرمانه باید در محل های امن نظیر کشو یا کمد های قفل دار نگهداری شوند. نباید هیچ گونه اطلاعات محرمانه ای در محل های باز و در دسترس در طول مدت عدم حضور، رها شوند.
- هر گونه گمان و حدس در مورد بروز نقص در امنیت و محرمانگی اطلاعات باید فوراً به مدیر واحد فناوری اطلاعات اطلاع رسانی شود.
- تأمین کنندگان خارج از سازمان باید به خاطر داشته باشند، ایشان نیز تحت همان قوانین امنیت اطلاعاتی هستند که کارکنان درون سازمان از آنها تبعیت می کنند.
- اطلاعات، بایگانی ها، فایل ها و نظایر آنها نباید در معرض دید بازدید کنندگان باشد، مگر اینکه بازدید کنندگان اختصاصاً مجاز به رویت اطلاعات باشند.
- اطلاعات در هر شکل و فرمتی باید در زمانی که دیگر مورد نیاز نیستند، به شیوه ای 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.

۱۵-۵- 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 پوشه ها و اطلاعات موجود در آنها تحویل و مدیر واحد دسترسی کلیه کارشناسان خود را در آن ثبت و سپس توسط واحد انفورماتیک این دسترسی ها بر روی اطلاعات موجود در سرور تهیه می شود.
- تغییر هر کدام از سطوح دسترسی بدون مجوز مدیر واحد امکان پذیر نیست.
- مسئولیت حذف یا دستکاری اطلاعات که در عملکرد واحد یا سازمان اختلال ایجاد کند، در واحد مربوطه بر عهده کارشناسان و مدیر واحد می باشد.

۱۶-۵- مدیریت حوادث امنیت اطلاعات

- حوادث امنیتی شامل (و نه محدود به) حملات ویروس ها، کرم ها، اسب های تروجان، استفاده غیرمجاز از دسترسی ها و تجهیزات نگهداری و پردازش اطلاعات و همچنین استفاده نادرست از آنها است.

تذکر:

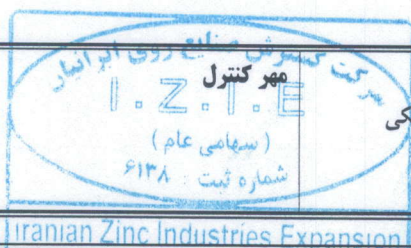
اسناد سیستم مدیریت یکپارچه (IMS) و روش اجرایی محرمانگی داده الکترونیکی فقط با مهر اصلی دارای اعتبار می باشد و تهیه کپی از اسناد مجاز نیست.



- هنگام بروز حوادث امنیتی، مدیر واحد فناوری اطلاعات در جلسه ای با مدیر عامل ضمن تشریح ابعاد حادثه در خصوص تشکیل تیم مقابله با حوادث (متشکل از مدیر واحد انفورماتیک و مدیران درگیر) تصمیم می گیرند.
 - 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 می کند:
 - الف- جلوگیری از حملات و دسترسی های غیرمجاز، علیه دارایی های اطلاعاتی سازمان.
 - ب- مهار خسارت های ناشی از ناامنی موجود در شبکه.
 - ج- کاهش رخنه پذیری به شبکه.
 - د- تأمین صحت عملکرد، قابلیت دسترسی و محافظت فیزیکی برای سخت افزارها و نرم افزارها، متناسب با حساسیت آنها.
 - ه- مدیریت فناوری اطلاعات باید در زمینه حوادث مختلف با دیگر سازمان های گروه در ارتباط باشد.
 - تمامی فعالیت های مشکوک که شامل (و نه محدود به) حوادث امنیتی احتمالی می شوند، می بایست به مدیریت انفورماتیک سازمان گزارش شوند.
- ۱۷-۵- دستگاه های قابل حمل و دور کاری**
- ۱-۱۷-۵- دستگاه های قابل حمل: این دستگاه ها شامل لپ تاپ، فلش، دوربین و موبایل و ... می باشد.
 - استفاده و انتقال دستگاه های قابل حمل با درخواست معاونت/مدیریت هر واحد و با مجوز صادره از واحد انفورماتیک امکان پذیر 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 می باشد.
 - به کارگیری دستگاه های شخصی برای تبادل اطلاعات شرکت ممنوع است.
 - انتقال اطلاعات غیرضروری و اضافی با لپ تاپ ها برای شرکت در جلسات برون سازمانی اکیداً ممنوع است و اطلاعات موردنیاز همان جلسه یا مأموریت با درخواست مدیر قسمت بر روی لپ تاپ قرار گیرد.
 - ۲-۱۷-۵- دور کاری:
 - بستر دور کاری بر حسب نیاز و کسب مجوز مدیر مربوطه برای کارشناسان و مدیران به وجود می آید.
 - برای دسترسی به سیستم ها و منابع داخلی از راه دور، استفاده از سیستم مدیریت دسترسی های ممتاز (PAM) الزامی است. این سیستم کلیه اتصالات را واسطه گری، ضبط و کنترل می کند.

تذکره:

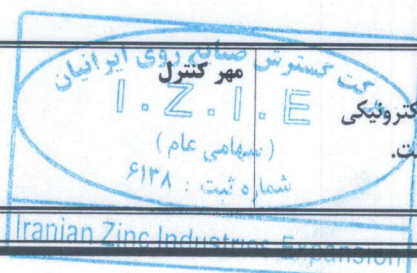
اسناد سیستم مدیریت یکپارچه (IMS) و روش اجرایی محرمانگی داده الکترونیکی فقط با مهر اصلی دارای اعتبار میباشد و تهیه کپی از اسناد مجاز نیست.



- در دورکاری، مجوز چک کردن ایمیل ها داده شده و تنظیمات آن را کارشناس واحد فناوری اطلاعات انجام می دهد.
- 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 دستگاه های انتقال داده شده در دورکاری توسط واحد انفورماتیک انجام شود.
- تحویل و برگرداندن سالم دستگاه ها 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.
- ۳-۱۷-۵ 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 پروتکل های قدیمی یا نرم افزارهای دسترسی مستقیم مانند RRAS، RDP یا AnyDesk ممنوع است.
 - کلیه افرادی که به وسیله PAM به شبکه سازمان دسترسی پیدا می کنند، باید به طور کامل از دارایی های 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 دسترسی های بعدی باید در اختیار واحد انفورماتیک قرار گیرد.
- ۱۸-۵ -نسخه پشتیبان (Backup)
 - نسخه پشتیبان شامل نسخه پشتیبان بانک های اطلاعاتی و دیتای سازمان و نسخه پشتیبان از تمامی سیستم عامل های سرورها است. مسئول تهیه نسخ پشتیبان کارشناس واحد انفورماتیک با نظارت مدیر واحد است.
 - کلیه اطلاعات سازمانی به صورت روزانه پشتیبان تهیه و این اطلاعات ۱ ماه بر روی سرور باقی بماند.
 - سیستم عامل سرورها ۱۵ روز یک بار باید نسخه پشتیبان داشته باشند و محل ذخیره سازی آنها روی سرور است.
 - در حال حاضر دیتای سرورها با نرم افزار Synology و سرورها با Veeam Backup نسخه پشتیبان تهیه شود.

تذکره:

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.



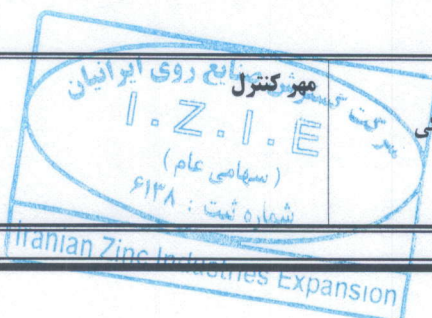
- کلیه نسخ پشتیبان باید بر روی رسانه ذخیره سازی مورد تأیید و در خارج از محل و در یک مکان با تدابیر امنیتی مناسب نگهداری شوند.
- در هنگام تهیه نسخ پشتیبان باید تطابق با نسخه اصلی صورت گیرد و از صحت اطلاعات آن اطمینان حاصل شود.
- رسانه های تاریخ گذشته، باید نابود شوند. در بازه های زمانی مشخص، قابلیت بازیابی 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 می شود.
 - 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.
 - ه- تاریخ مصرف نسخه پشتیبان.
 - و- برای نسخه پشتیبان رمز تعریف گردد.
 - ز- خارج نمودن نسخ پشتیبان از سازمان به صورت ماهانه صورت گیرد.
 - ح- مسئولیت نگهداری از نسخ پشتیبان در خارج از سازمان تحت عنوان نسخ آرشیو بر عهده معاونت اداری/مالی است.
- به منظور 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 نرم افزار آکرونیس اطلاعات برگردانده شود.
- سیستم عامل های دارای مشکل نیز روی سرورها با نرم افزار Veeam برگردانده شود.
- اطلاعات بانک اطلاعاتی نیز که روی دیسک های بلوری ذخیره می شوند، با قابلیت خود نرم افزار SQL برگردانده شوند.

۱۹-۵- امنیت فیزیکی و محیطی

- ۱۹-۵-۱- دسترسی به تأسیسات اطلاعاتی: امنیت فیزیکی کلیه کامپیوترها و تجهیزات ارتباطی که متعلق به سازمان یا توسط سازمان مورد استفاده قرار می گیرند، باید توسط تمامی کارکنان، مدیران، تأمین کنندگان، کارکنان پاره وقت، کارکنان موقت، کارآموزان و دیگر کارکنانی را که مجاز به دسترسی به سیستم های اطلاعاتی سازمان شناخته اند، مورد توجه قرار گیرد.
 - دسترسی فیزیکی به محدوده های کنترلی (محدوده هایی که در آنها سیستم های اطلاعاتی یا اطلاعات حساس نگهداری می شوند، نظیر اتاق سرورها) می بایست مدیریت و ثبت شوند.

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.



- تمامی محدوده های کنترلی می بایست نشانه گذاری و برچسب زده شوند و به تناسب حساسیت و اهمیت عملکردشان مورد حفاظت فیزیکی قرار گیرند.
- دسترسی به محدوده های کنترلی می بایست صرفاً برای کارکنان و تأمین کنندگان مجاز شناخته شود که مسئولیت کاریشان نیازمند دسترسی به محدوده مورد نظر است.
- درخواست برای دسترسی می بایست طبق روش اجرایی برقراری دسترسی صورت پذیرد.
- روش اجرایی دسترسی احتمالی برای محدوده های کنترلی می بایست آماده و در مواقع از کار افتادن سیستم کنترل خودکار دسترسی مورد استفاده قرار گیرد.
- کارت های دسترسی و یا کلیدها نمی بایست به صورت اشتراکی مورد استفاده قرار گیرند یا به دیگران قرض داده شوند.
- کارت های دسترسی یا کلیدهایی که دیگر مورد نیاز نیستند، می بایست به مسئول محدوده کنترلی برگردانده شوند. کارت ها نباید بدون طی مراحل بازگرداندن، به افراد دیگر اختصاص یابد.
- دسترسی بازدیدکنندگان به محدوده های کنترلی می بایست 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 رک ها الزامی است.
 - کنترل دمای اتاق در دمای ۲۰ درجه سانتی گراد 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 -کنترل های مداخل فیزیکی: کلیه مداخل فیزیکی باید مجهز به قفل و دوربین های مدار بسته باشد.
- ۵-۱۹-۵ -امن سازی دفاتر، اتاق ها و امکانات: باید محل های سرورها ایزوله و به جز مسئولین واحد فناوری اطلاعات کسی اجازه دسترسی به سرورها و سوییچ ها 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 ذخیره سازی.
 - مصادیق اقدام انسان- تصادفی (A) مانند نقص در سیستم تهویه، نقص در سخت افزار، اشکال در تعمیرات، اشکال در نرم افزار، استفاده از نرم افزار توسط افراد غیرمجاز، استفاده از نرم افزار به شیوه ای



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.

تذکر:

غیرمجاز، استفاده از نرم افزار 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، آتش افروزی، آسیب عمدی، دزدی، استفاده غیرمجاز از محیط ذخیره سازی، تغییر هویت و جعل هویت، نرم افزارهای 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 سر باز زدن، استفاده نادرست از منابع.

○ کلیه سرورها و یو پی اس ها و آنتن ها با تهدیدهای موجود در جدول باید کنترل شوند. این مسئولیت بر عهده واحد انفورماتیک می باشد.

• ۵-۱۹-۷ - امنیت کابل کشی: کلیه کابل کشی ها باید چک و اگر آسیب یا نقصی در کابل کشی هست باید توسط واحد انفورماتیک تعمیر شود. این کابل کشی شامل کابل کشی شبکه و تلفن می باشد.

• ۵-۱۹-۸ - خروج دارایی ها: تجهیزات، نرم افزارها 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 دارایی های خارج از محوطه: امنیت تمام دارایی های درون پروژه ها بر عهده مدیر پروژه می باشد.

• ۵-۱۹-۱۰ - امحا یا استفاده مجدد از تجهیزات به صورت امن:

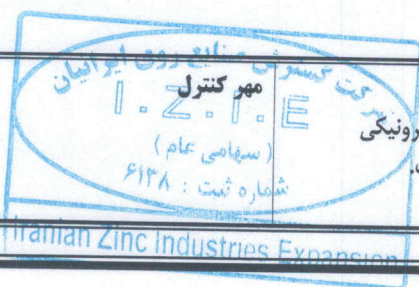
○ نرم افزارهای زیادی وجود دارند که می توانند برای بازیابی فایل ها و اطلاعات حذف شده از روی تجهیزات سخت افزاری (فرمت شده) مورد استفاده قرار گیرند. برای کاهش احتمال خطر انتشار بدون مجوز اطلاعات حساس و محرمانه، می بایست اطلاعات موجود بر روی تجهیزاتی که پیشتر مورد استفاده قرار گرفته اند، به طور امن حذف شوند. پس از این عملیات، بازیابی اطلاعات توسط نرم افزارهای معمولی امکان پذیر نخواهد بود و برای بازیابی می بایست تکنیک های تخصصی به کار گرفته شوند. همچنین برای حذف اطلاعات می توان از روش هایی استفاده نمود که بازیابی توسط تکنیک های تخصصی نیز امکان پذیر نباشد.

○ تمامی اطلاعات سیستم های کامپیوتری و رسانه های مرتبط با آنها که ممکن است حاوی اطلاعات حساس یا محرمانه باشند، می بایست پیش از استفاده مجدد یا انهدام، پاک شوند.

○ اطلاعات تمامی بسترهای ذخیره سازی اطلاعات سیستم ها و قطعاتی که در سازمان مجدداً مورد استفاده قرار می گیرند، باید با یک نرم افزار مورد تأیید پاک شوند. در برخی از موارد باید از سیستم ها پیش از استفاده مجدد یک نسخه پشتیبان کامل تهیه شود.

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.



- تمامی بسترهای ذخیره سازی سیستم ها و تجهیزاتی که مورد استفاده مجدد قرار گرفته، فروخته، یا بخشیده می شوند، یا حتی به عنوان وسایل غیرقابل استفاده به بیرون از سازمان منتقل می شوند، لازم است توسط نرم افزار مورد تأیید پاک شوند.
 - تمامی عملیات پاک کردن یا انهدام تجهیزات می باید با اطلاعات زیر ثبت شوند: تاریخ و زمان عملیات، نام، عنوان و امضای کارشناس مربوطه، شرح اقدامات انجام گرفته.
 - ۱۱-۱۹-۵-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 شناخته اند، ضروری است.
 - کاربران ایستگاههای کاری نباید هیچ دستگاه جانبی که فاقد تأییدیه واحد انفورماتیک است را به ایستگاههای کاری متصل کنند.
 - مانیتورهای ایستگاههای کاری می بایست به گونه ای قرار گیرند که از دیده شدن اطلاعات حساس توسط افراد غیرمجاز جلوگیری شود.
- ۲۰-۵-امنیت سیستم تلفنی ویپ
- در راستای حفظ محرمانگی و جلوگیری از شنود، دستکاری و سوءاستفاده از سیستم تلفنی سازمان، موارد زیر رعایت گردد:

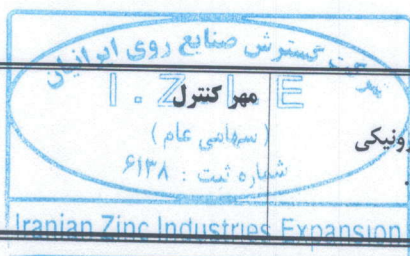
- راه اندازی سیستم VoIP فقط توسط واحد فناوری اطلاعات و روی زیرساخت امن صورت گیرد.
- تمامی ارتباطات VoIP باید از طریق VPN داخلی یا VLAN مجزا منتقل شوند.
- استفاده از SIP-TLS و SRTP برای رمزگذاری سیگنالینگ و مکالمات الزامی است.
- دسترسی به پنل مدیریت مرکز تلفن (PBX/IPPBX) فقط برای مدیر IT مجاز است.
- اتصال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

۲۱-۵-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 امکان پذیر است.

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.



- ذخیره سازی اطلاعات سازمان روی فلش، هارد اکسترنال، CD/DVD، موبایل و لپ تاپ شخصی ممنوع است.
 - ارسال فایل از طریق ایمیل شخصی، پیام رسان ها، شبکه های اجتماعی، وب سرویس های ذخیره سازی (Google Drive)، Dropbox و ... ممنوع است.
 - هرگونه عکس برداری یا فیلم برداری از صفحه نمایش، مانیتور یا سیستم ها بدون مجوز مدیریت ممنوع است.
 - فایل های حساس فقط باید روی سرور داخلی و با سطح دسترسی کنترل شده 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.
- ۵-۲۲- بازدید دوره ای اتاق سرور، برق، کولینگ و سنسورها**
- در راستای افزایش پایداری عملیاتی و کاهش ریسک های محیطی:
 - واحد IT موظف است حداقل ماهانه یکبار بازدید کامل اتاق سرور را انجام دهد.
 - موارد زیر باید در چک لیست بازدید ثبت و نگهداری شود:

○ الف) سیستم برق

- عملکرد صحیح UPS، برق ورودی، تثبیت کننده ها و باتری ها
- 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 رک ها، قفل بودن درب ها و وضعیت کابل کشی



تذکره:

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.

- 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.
- پروتکل های مجاز شامل OpenVPN، L2TP/IPSec یا SSL-VPN با رمزنگاری قوی هستند.
- هرگونه دسترسی ریموت بدون VPN رسمی سازمان ممنوع است.
- کلید تونل های VPN باید دارای موارد زیر باشند:
 - احراز هویت دو مرحله ای (2FA)
 - گواهی دیجیتال معتبر (Certificate-Based Authentication)
 - رمزگذاری AES-256
- دسترسی VPN برای کاربران موقت باید زمان دار 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 می شود.
- تمام ترافیک VPN باید از فایروال مرکزی عبور کند و تحت پایش قرار گیرد.

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.

