۱- هدف

این آیین نامه با هدف حفظ امنیت و صحت اطلاعات ، استفاده‌ی 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، دسترس پذیری در زمان ایجاد و انتقال و نگهداری است.

۲- کلیات

- اطلاعات سازمان صرفا توسط افراد مجاز قابل دسترسی باشند.
- محرمانگی اطلاعات همواره در کل سازمان همچنین در پروژه ها ،بین واحدهای سازمانی حفظ شود.
- در کلیه فرایندها امنیتی یکپارچگی اطلاعات حفظ شود.
- پیاده سازی سیاستهای امنیتی نباید اختلالی در روند کاری سازمان و واحدها ایجاد کند.
- آموزشهای لازم را در مورد امنیت اطلاعات و سیاست های امنیتی به کل سازمان داده شود
- تمامی رخنه های امنیت اطلاعات و ضعف های احتمالی توسط همه کاربر ان گزارش شده و به آنها رسیدگی گردد.
- تبادل اطلاعات بین سازمانی همواره ازطریق کانالهای مجاز و تایید شده سازمان صورت گیرد.
- تمام دستورالعمل های امنیتی اتخاذ شده برای کلیه سازمان یکسان است و موارد استثنا ، تنها در صورت دستور کتبی مدیریت ارشد اعمال می شود.
- هر گونه 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 بکارگرفته شود.
- کلیه معاونین / مدیران به صورت مستقیم مسئول اجرای دستورالعمل های امنیتی مربوط به واحد خود هستند.
- آیین نامه و دستورالعمل های امنیتی مندرج در آن توسط مدیریت ارشد سازمان تایید می شود و به طور سالیانه مورد بازنگری قرار گیرد.
- اجرای آیین نامه امنیت اطلاعات بطور دوره ای متناسب با هر دستورالعمل پایش می شود.
- هر کاربر در شبکه فقط مجاز است به اطلاعاتی دسترسی داشته باشد که از طرف مدیران مافوق برای او مجاز تشخیص داده شده است . و هر گونه تلاش برای دسترسی به اطلاعاتی خارج از حیطه تعیین شده (اعم از مشاهده ، تغییر ، دستکاری و ...) اکیدا ممنوع بوده و تخلف محسوب می‌شود.
- اختلال در عملکرد شبکه و کاربران اکیدا ممنوع است.
- از اقداماتی که منجر تخریب اطلاعات شود، پرهیز شود.
- هرگونه تلاش جهت نفوذ به سایر کلاینتها ، سرورها و دیتابیسها ، که جزء دسترسی مجاز یک کاربر نمی باشد توسط هر گونه ابزار سخت افزاری یا نرم افزاری که باشد تخلف محسوب می شود..

۳- دامنه کاربرد

این آیین نامه کلیه اطلاعات سازمان اعم از اطلاعات تولید شده در داخل شرکت رشد صنعت و اطلاعات مربوط به کار فرمایان و سیستم های کامپیوتری و تجهیزاتی که به شبکه متصل و درون سازمان هستند و نیز سیستم هایی که با نام سازمان در خارج از شرکت هستند(مانند پروژه ها) و همچنین کلیه کاربران داخلی و خارج شبکه که با سیستم های سازمان در گیر هستند را شامل می شود.

۴- تعاریف

- **اطلاعات**: داده های پردازش شده که مبنایی برای تصمیم گیری می باشندو شامل تمامی اطلاعات دیجیتالی **شرکت رشد صنعت** ، اعم از متون ، نقشه ها ، تصاویر ، نامه ها ، پرونده ها ، اسناد ، فایلهای کامپیوتری ، اطلاعات توصیفی و جغرافیایی و ... چه داخل شبکه و سرورها چه برروی کلاینتها و کامپیوترهای مستقل است . اطلاعات یک دارایی است که همانند سایر دارایی های باید حفظ و نگهداری شود.

اطلاعات شامل:

- مستندات الکترونیکی
- مراسلات متداول
- رسانه های الکترونیکی
- سوابق پایگاه داده
- ایمیل ها
- CD ROM ها، DVD ROM ها، نوارها و ...
- فیلم ها
- اطلاعات بیان شده در جلسات

کاربران: معاونین ، مدیران ، کارشناسان ، پیمانکاران مرتبط با شبکه و سایر کاربرانی که به نحوی با بخش های مدیریتی و یا کاربردی درون سازمانی شبکه در ارتباط می باشند .

نرم افزار : شامل سیستم عامل ها مانند Linux و Windows ، نرم افزارهای کاربردی عمومی مانند Office ، نرم افزارهای کاربردی سازمانی مانند سیستم اتوماسیون اداری ، نرم افزارهای کاربردی اختصاصی مانند سیستم های فنی و مهندسی ، نرم افزارهای مدیریت شبکه و سیستم های تحت وب مانند Active Directory، kerio mail، SQL Server، My SQL، Kerio Server و ...

سخت افزار: شامل ایستگاه های کاری ، سرویس دهنده ها Data Projector ها، PC ها ، Laptop ها ، تجهیزات شبکه و انتقال داده مانند Router ها ، Switchها ، Hub ها و ... چاپگرها ، پویشگرها ، تجهیزات سیار انتقال اطلاعات مانند Flash Memory ها ، CD ها ، DVD ها ، دوربین های دیجیتالی ، و ...

ارتباطات : شامل کابل های فیبرنوری ، ۵CAT و ۶CAT ، ارتباطات شبکه سازمان با سایر شبکه های موجود از قبیل شبکه سایر کارخانجات و دفتر مرکزی ، شبکه اینترنت و ...

کاربر مجاز : تمام کاربرانی که با تایید بخش اداری و با توجه به پروسه جذب در سازمان احراز هویت گردیده اند و دارای نام کاربری در دامنه سازمان می باشند.

کاربر مجاز موقت : تمام کاربرانی که با تایید 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 هستند که از سازمان های بیرونی به سازمان رشد صنعت سرویس می دهند.این کاربران دارای دسترسی به Remote Desktop ، public user و DBA User بانک اطلاعاتی با توجه به نام کاربری تعریف شده ، هستند.

۵– مسئولیت ها و اختیارات

- **مدیر عامل :** مسئول تصویب و ابلاغ آیین نامه امنیت اطلاعات به همه واحد های شرکت رشد صنعت است.
- **مدیر انفور ماتیک :** مسئول تدوین به روزآوری، و نظارت برحسن اجرای این آیین نامه در واحد انفور ماتیک و کلیه واحد های سازمان و همچنین بازنگری و بهبود آن در مقاطع مقتضی است. همچنین مسئولیت مدیریت فنی سایت شرکت رشد را داراست
- **معاونین ومدیران واحدها:** مسئول نظارت بر حسن اجرای این آیین نامه در واحد تحت مدیریت خود هستند.
- **مدیران پروژه ها :** مسئول اجرای این آیین نامه در تمام مقاطع اجرای پروژه ای که مدیریت آن را به عهده دارند، و در تمام واحد های در گیر هستند.
- **کاربران:** مسئول اجرای این آیین نامه هستند.
- **مدیر سیستم ها و روش ها:** مسئول پایش اجرای این آیین نامه و گزارش آن به مدیر عامل در مقاطع مقتضی است.
- **مشاور انفور ماتیک :** مسئول همکاری با مدیر واحد انفورماتیک در پیاده سازی و انتخاب سخت افزار و نرم افزار مناسب و همچنین ارائه پیشنهادات بهبود است .
- **مدیر توسعه بازار:** مسئول مدیریت محتوای وب سایت شرکت است.

۶– امنیت اطلاعات

– دستور العمل ها

۶-۱- پست الکترونیکی

۶-۲- اطلاعات ذخیره شده در سرور

۶-۳- نرم افزار ERP

۶-۴- اطلاعات اکتیو دایرکتوری

۶-۵- اطلاعات مربوط به سایت سازمان

۶-۶- اطلاعات مربوط به دامنه و هاست سازمان

۶-۷- اطلاعات مربوط نرم افزار PWKARA

۶-۸- اینترنت

۶-۹- حفاظت در برابر ویروس ها

۶-۱۰- اطلاعات دوربینها

۶-۱۱- سرورها

۶-۱۲- ارسال / دریافت اطلاعات ازکارفرما /پیمانکار

۶-۱۳- نگهداری و اداره اطلاعات محرمانه

۶-۱۴- امنیت اطلاعات در مدیریت پروژه

۶-۱۵- سطوح دسترسی

۶-۱- پست الکترونیکی

۶-۱-۱-ایمیل های سازمانی: معرفی و ایجاد ایمیل های سازمانی توسط کارشناسان IT با نظر مدیران هر واحد انجام می شود.

۶-۱-۲-ایمیل های شخصی:

استفاده متعارف از منابع سازمان برای ایمیل های شخصی پذیرفتنی است، ولی ایمیل های غیر مرتبط با کار می‌بایست در پوشه جداگانه و مجزا از ایمیل های کاری نگهداری شوند.درضمن ایمیل های شخصی باید از ایمیل های سازمانی جدا و ایزوله 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 ایمیل ها بپردازد.

دستورالعمل:

- فایل نگهداری ایمیل های سازمانی تنها در دسترس خود کاربر و کارشناس IT می باشد.
- از تمامی ایمیل هایی که حاوی اطلاعات سازمانی هستند بطور روزانه، نسخه پشتیبان تهیه شده و در سرور نگهداری می شوند.
- ارسال ایمیل سازمانی برای خارج از شرکت اعم از کارفرمایان، تامین کنندگان و سایر اشخاص حقیقی تنها توسط مدیران و پست های سازمانی معرفی شده توسط ایشان انجام می شود. لیست تایید شده افراد مجاز نزد واحد انفورماتیک شرکت نگهداری می شود .

۶-۲- اطلاعات ذخیره شده در سرور

۶-۲-۱- 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.

۶-۲-۲- اطلاعات فردی:

کلیه اطلاعات کاربران سازمان روی سرور ذخیره می شود. اطلاعات فردی در درایو p هر سیستم قابل مشاهده است.

دستورالعمل:

- کاربران از قرار دادن اطلاعات سازمانی در درایو P خودداری کنند.
- اطلاعاتی که کاملا شخصی است .نباید در سیستم نگهداری شود.
- مسئولیت پاک شدن اطلاعات فردی بر عهده کاربر است.
- قراردادن فایلهای Multi Media و عکس در درایو P 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 فایلهای مهم باید پسورد داشته باشند.

۶-۳- نرم افزار ERP

- نرم افزار ERP شامل سیستمهای مالی ، منابع انسانی، انبار ، حقوق و دستمزد ، اموال و .... ، دارای زیر سیستمهای مختلفی است که کاربر هر واحد با توجه به مجوز صادر شده از طریق معاونت اداری و مالی به آن دسترسی دارد. این نرم افزار دارای سطوح دسترسی مختلفی است که مسئولیت اجرای مجوز به عهده مدیر انفورماتیک است . کلیه اطلاعات این نرم افزار بر روی سرور نگهداری می شود.
- در صورت لزوم تبادل اطلاعات (ریپلیکیشن بین سرورها)بین سرورهای دفتر مرکزی جهت به روز رسانی اطلاعات مربوط به سیستم ERP و پروژه ها ی سازمان انجام می شود.

دستورالعمل:

- 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 سرور ها بر عهده مدیر IT است.
- کارکرد درست روترها و ریپلیکیشن به منظور برقرای درست ارتباط بطور مستمربایدکنترل وچک شود.
- دستورات پینگ برای ارتباط با روتر دفتر مر کزی و پروژه ها و شرکت های مشارکت کننده باید کنترل شود.
- در صورت قطع شدن ارتباط ، تمامی آی پی آدرسهای ارتباط بین دو نقطه کنترل می شود.

۶-۴- اطلاعات مربوط به اکتیو دایرکتوری

- تعریف /حذف کاربران و رمزهای کاربران، اطلاعات مربوط به پروفایلهای آنها ، ایجاد دسترسی ها و مدیریت سرور DNS ،DHCP به عهده مدیر انفورماتیک است.

۶-۴-۱- رمز عبور:

دستورالعمل:

- رمز عبور هرکاربر باید حدوداً هر ۶ 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 ی واگذاری نام کاربری و رمز عبور خود به دیگران را ندارند. (استفاده غیر مجاز از USB)

- رمز عبور کاربران باید حداقل از ۶ 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 mnop یا ۱۲۳۴۵
- در رمز عبور نباید از نام یا نام خانوادگی فرد استفاده شود.
- تغییر در رمز عبور به اطلاع مدیر مستقیم کاربر برسد.

۶-۴-۲- ایجاد و مدیریت دسترسی کاربران

دستورالعمل:

- کلیه دسترسی ها به اطلاعات مرتبط با حوزه کاری کاربر باید با درخواست مستند پس از تایید توسط مدیر مستقیم ایجاد می شوند.
- کلیه دسترسی ها به اطلاعات غیر مرتبط با حوزه کاری کاربر باید با درخواست مستند پس از تایید توسط مدیر مستقیم و معاونت اداری و مالی ایجاد شوند، بدیهی است که درخواست های تایید 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 ۳۰ روز از کد کاربری خود استفاده نکنند ، غیر فعال 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 هردلیلی قطع همکاری با سازمان دارند باید نام کاربریشان در سیستم به مدت دو ماه غیرفعال وپس از آن حذف شود.
- کلیه تعاریف حق دسترسی با ید توسط واحد انفورماتیک کنترل و اجرا می شود.

۶-۵- اطلاعات مربوط به سایت

دستورالعمل:

- مدیریت کنترل پنل و هاست سایت توسط کارشناسIT با نظارت مدیر انفورماتیک انجام می شود.
- اطلاعات سایت بطور مستمر به روز رسانی شود.
- در جهت بالا بودن سایت از نظر رتبه بندی تلاش شود.

۶-۶- اطلاعات مربوط به دامنه و هاست سازمان

مدیریت اطلاعات کاربران برروی هاست و دامنه به عهده واحد انفورماتیک است.

۶-۷- اطلاعات مربوط به ورود و خروج در نرم افزار PWKARA

این نرم افزار جهت ثبت ورود و خروج کاربران استفاده می شود و واحد اداری مسئولیت استفاده از این نرم افزار را دارد. واحد انفورماتیک وظیفه ایجاد امنیت براساس این آیین نامه را برای اطلاعات این سیستم برعهده دارد.

دستورالعمل:

- نام کاربری و رمز عبور توسط کارشناس انفورماتیک ثبت می شود و دسترسی های لازم به پرسنل داده می شود.
- دسترسی کامل به این برنامه تنها در اختیار مسئول اداری و دسترسی مدیران سایر واحدها در حد مشاهده کارکرد پرسنل زیرمجموعه است .

۶-۸- اینترنت

از اینترنت در سازمان در جهت به دست آوردن اطلاعات مفید و سودمند در جهت بهبود انجام مسئولیت و ارسال ایمیل و ... استفاده می شود.

دستورالعمل:

- مدیر هر واحد ، میزان استفاده از اینترنت توسط کارکنان آن واحد را مشخص می کند.
- استفاده از اینترنت برای انجام کارشخصی ممنو ع است.
- نصب و بکارگیری نرم افزارهایی که به اینترنت نیاز دارند باید با مجوز مدیریت هر دپارتمان انجام می شود.
- میزان استفاده کاربران از اینترنت بطور ماهانه به مدیریت ارشد گزارش می شود.
- هر کاربر تنها با نام کاربری و کلمه عبور خود می تواند وارد اینترنت شود.
- رمز وایرلس فقط در اختیار مدیران قرار داده می شود و فقط با تعریف مک ادرس یکدستگاه همراه امکان اتصال به وایرلس وجود دارد و سایر کاربران در سازمان مجاز به استفاده از شبکه وایرلس نمی باشند مگر با تشخیص مدیریت واحد و بصورت محدود در زمان معین (این زمان بیشتر از مدت یک روز کاری نمی تواند باشد)
- کاربران مجاز به استفاده از اینترنت وایر لس حق انتقال رمز را به سایر کارکنان ندارند.
- درصورت بکارگیری اینترنت وایرلس با توجه به محرمانگی اطلاعات ، ورود به شبکه تحت هیچ شرایطی امکان پذیر نمی باشد.

۶-۹- حفاظت در برابر ویروس ها

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

دستورالعمل:

- کلیه کامپیوترهایی که به سازمان تعلق دارند و یا توسط سازمان مدیریت می شوند، همینطور Laptop هایی که به شبکه سازمان متصل می شوند و یا به صورت مستقل مورد استفاده قرار می گیرند، می بایست از نرم افزار آنتی ویروس و تنظیمات مورد تایید واحد انفورماتیک سازمان استفاده کنند.
- تمامی کامپیوترهایی که به سازمان تعلق ندارند و یا تحت مدیریت سازمان نمی باشند، پیش از هرگونه ارتباط و اتصال به منابع اطلاعاتی سازمان، می بایست از نرم افزار ضد ویروس و تنظیمات مورد تایید مدیر انفورماتیک سازمان استفاده کنند.
- نرم افزار ضد ویروس نباید غیر فعال (Disable) شود.دسترسی کاربران به این گزینه امکان پذیر نیست.
- تنظیمات نرم افزار ضد ویروس نباید به گونه ای تغییر کند که قابلیت تاثیرگذاری آن را کاهش دهد.
- تنظیمات به روز رسانی نرم افزار ضد ویروس نباید به گونه ای تغییر کند که بازه های زمانی به روز رسانی آن را کاهش دهد.
- هر سرویس دهنده ای که به شبکه سازمان متصل است، باید از نرم افزار ضد ویروس مورد تایید سازمان استفاده کند.

- تمامی گذرگاه های پست الکترونیکی باید از نرم افزار ضد ویروس مورد تایید 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 انفورماتیک گزارش داده شود.
- کارشناس انفورماتیک باید به روز رسانی آنتی ویروس را چک کند و در صورت مشکل باید با شرکت موردنظر تماس برقرار کند.

۶-۱۰- دوربین ها

مدیریت وکنترل دوربین ها وکلیه اطلاعات مربوط به نرم افزار دوربین ها شامل نام کاربری و کلمه های عبور ، نرم افزار نصب، همچنین معرفی کاربرانی که مجاز به دیدن فیلم ها هستند نیز ،با واحد انفور ماتیک است.

دستورالعمل:

- نرم افزار دوربین ها حتما در سرور و نسخه کلاینت آن در کامپیوترهای کاربران مجاز نصب می شود
- فیلم ضبط شده دوربینها در سرور نگهداری می شود و این اطلاعات ذخیره شده باید چک شود.
- فیلم دوربینها بسته به تعداد دوربینها به مدت ۳۰ روز نگهداری می شود.
- به جز مدیران و افراد معرفی شده توسط آنها هیچکس حق دیدن فیلمهای ضبط شده را ندارد.
- در صورت ضرورت مشاهده فیلمهای ضبط شده برای شخص موردنظر باید مجوز مدیریت ارشد یا مدیر قسمت صادر شود.

۶-۱۱- سرورها

مدیریت وکنترل سرورها وکلیه تجهیزات مربوطه از حیث آماده بکاری سرویس های سازمان بمنظور دردسترس قرار داشتن همیشگی شبکه و اطلاعات بر عهده واحد انفور ماتیک می باشد.

دستورالعمل

- تامین به موقع قطعات یدکی مصرفی در سرورها مانند (هارد دیسک ،پاور ماژول ،رم و غیره...) انجام شود.
- سرورها بصورت دوره ای هر ۶ماه 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 تامین شود.
- بروزرسانی سخت افزار سرورها براساس نیازهای سازمانی بطور ۳ سالانه بررسی شود.
- نرم افزارهای سرورها جهت افزایش امنیت و بستن حفره های امنیتی بروزرسانی شوند.
- سرویس کلاسترینگ جهت راه اندازی خودکار سرور پشتیبان در مواقع بروز نقص فنی برای سرور اصلی سازمان باید در هر زمان آماده بکار باشد.

۶-۱۲- ارسال / دریافت اطلاعات ازکارفرما /پیمانکار و ...

دستورالعمل

- استاندارد نحوه ارسال اطلاعات مشخص شده 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 تعیین شده توسط مدیر هر واحد انجام شود.
- ارسال اطلاعات باید ترجیحا درقالب فایلهای 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 شده و پس از تایید سلامت بکار گرفته شوند.
- استفاده از نرم افزارهای ارتباط جمعی مانند اینستاگرام ،واتزآپ و ... در سازمان ممنوع می باشد .

۶-۱۳- مدیریت اطلاعات

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 است که توسط کارمندان، اعضاء، مدیران، پیمانکاران، کارمندان پاره وقت و موقتی و دیگر کارمندانی که مجاز به دسترسی به اطلاعات سازمان همچنین کاربران تایید شده ای که خارج از شبکه هستند، مورد استفاده قرار می گیرند. باید حفظ شود.

دستورالعمل:

- اطلاعات نباید از طریق سیستم هایی که به سازمان تعلق ندارند، مورد استفاده قرار گیرند و یا روی آنها ذخیره شوند، مگر این که مجوز های 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 غیر ضروری خود داری شود.
- تاییدیه شماره فکس و فکس حتما دریافت شود.(در صورت امکان جهت کاهش احتمال خطا از شماره گیر برنامه ریزی شده استفاده شود.)
- 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 تعیین شده توسط مدیر هر واحد انجام شود.
- وقتی هر یک از کارکنان میزو 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.
- هرگونه گمان و حدس در مورد بروز نقص در امنیت و محرمانگی اطلاعات باید فورا به مدیر انفورماتیک اطلاع داده شود.
- پیمانکاران خارج از سازمان باید به خاطر داشته باشند، ایشان نیز تحت همان قوانین امنیت اطلاعاتی هستند که کارمندان درون سازمان از آنها تبعیت می کنند.

- اطلاعات، بایگانی ها، فایل ها و نظایر آنها نباید در معرض دید بازدید کنندگان باشد، مگر این که بازدیدکنندگان اختصاصا مجاز به مشاهده اطلاعات باشند.
- اطلاعات در هر شکل و فرمتی می بایست 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 جدا شده، پیگیری می شود و ممکن است منجر به اقدامات قانونی شود.

۶-۱۴- امنیت اطلاعات در مدیریت پروژه:

مسئولیت امنیت اطلاعات در مدیریت پروژه ها صرف نظر از نوع پروژه به عهده مدیر پروژه است.

دستورالعمل

- ارسال کلیه سیستم ها و نرم افزار ها ودستگاه هایی به محل اجرای پروژه موردنظر باید با تایید و مجوز معاونت پروژه ها، و نظارت واحد انفورماتیک انجام شود.
- انتقال اطلاعات لازم باید با مجوز مدیریت پروژه انجام شود.
- حفظ امنیت اطلاعات در محل اجرای پروژه به عهده مدیر پروژه است.
- صدور مجوز استفاده از فلش و رایتر برای دستگاه های ارسالی به محل اجرای هر پروژه به عهده مدیر همان پروژه است.
- محرمانگی اطلاعات در پروژه باید براساس "آیین نامه امنیت اطلاعات "حفظ شود .

۶-۱۵- سطوح دسترسی:

سطح دسترسی هر کاربر به اطلاعات با توجه به چارت سازمانی و مجوز مدیر واحد و دستور مدیر واحد انفورماتیک تعریف می شود.

دستورالعمل:

- فایل آماده شده توسط واحد انفورماتیک به مدیر واحد جهت مشخص کردن نام پوشه ها و اطلاعات موجود در آنها تحویل داده می شود و مدیر واحد دسترسی کلیه کارشناسان خود را در آن ثبت می کند 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 و یا دستکاری اطلاعات که در عملکرد واحد یا سازمان اختلال ایجاد کند در واحد مربوطه بر عهده کارشناسان و مدیر واحد می باشد.

۷- مدیریت حوادث امنیت اطلاعات

حوادث امنیتی شامل (و نه محدود به) حملات ویروس ها، کرم ها، اسب های تراوا، استفاده غیر مجاز از دسترسی ها و تجهیزات نگهداری و پردازش اطلاعات و همچنین استفاده نادرست از آنها به صورتی که در دستورالعمل استفاده قابل قبول از تجهیزات نگهداری و پردازش اطلاعات ذکر شده است، می باشد.

دستورالعمل:

- هنگام بروز حوادث امنیتی مدیر انفور ماتیک در جلسه ای با مدیر عامل ضمن تشریح ابعاد حادثه در خصوص تشکیل تیم مقابله با حوادث (متشکل از مدیر واحد انفور ماتیک و مدیران درگیر) تصمیم می گیرند.
- مدیر واحد انفورماتیک ، مدیریت و راهبری تیم مقابله با حوادث را برعهده دارد.
- تیم مقابله با حوادث طبق "دستورالعمل مدیریت حوادث " اهداف ذیل را دنبال می کند:
  - جلوگیری از حملات و دسترسی های غیر مجاز ، علیـه دارایی های اطلاعاتی سازمان
  - مهار خسارت های ناشی از نا امنی موجود در شبکه
  - کاهش رخنه پذیری به شبکه
  - تامین صحت عملکرد ، قابلیت دسترسی و محافظت فیزیکی برای سخت افزارها و نرم افزارها، متناسب با حساسیت آنها .
- مدیریت فناوری اطلاعات باید در زمینه حوادث مختلف با دیگر سازمانهای 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 داده شوند.
-

۸- دستگاههای قابل حمل و دورکاری

۸-۱- دستگاههای قابل حمل:

این دستگاهها شامل لپ تاپ، فلش، دوربین و موبایل و ... می باشد.

دستورالعمل:

- استفاده و انتقال دستگا ه های قابل حمل بادرخواست معاونت / مدیریت هر واحد و با مجوز صادر شده 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 و یا تبلت به سیستم و شبکه سازمان ممنوع می باشد.
- بکارگیری دستگاههای شخصی برای تبادل اطلاعات شرکت ممنوع است.
- انتقال اطلاعات غیر ضروری و اضافی با لب تاپ ها برای شرکت در جلسات برون سازمانی اکیدا ممنوع است و اطلاعات موردنیاز همان جلسه یا ماموریت با درخواست مدیر قسمت بروی لب تاپ قرار گیرد.

۸-۲- دورکاری:

بستر دورکاری برحسب نیاز و کسب مجوز مدیر مربوطه برای کارشناسان و مدیران به وجود می آید، و با در اختیار گذاشتن یک دستگاه لب تاپ سازمانی و بکارگیری سرویس RRAS اجرایی می شود. در دورکاری مجوز چک کردن ایمیلها داده می شود و تنظیمات آن را کارشناس انفورماتیک انجام می دهد . در موارد خاص و کمبود منابع از سرویس AnyDesk دورکاری با رعایت ضوابط امنیتی دورکاری اجرا می شود.

درصورت نیاز به دسترسی به اطلاعات درون سازمان باید تمهیدات لازم اندیشیده شده و با درخواست مدیر واحد و مجوز مدیر ارشد سازمان انجام شود.

دستورالعمل:

- کلیه تنظیمات مربوط روی دستگاههای انتقال داده شده در دورکاری توسط واحد انفورماتیک انجام می شود.
- تحویل و برگرداندن سالم دستگاهها از دورکاری بر عهده کاربر مربوطه می باشد.
- 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.

۸-۳- اتصال از راه دور به شبکه داخلی

دستورالعمل

- کارکنانی که مجوز دسترسی به صورتRRAS , Any Desk را دارند نباید این مجوز را در اختیار سایر کارکنان قرار دهند. کلیه افرادی که بوسیله RRAS , Any Desk به شبکه سازمان دسترسی پیدا میکنند 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 کاربر از سیستم غیر فعال شود.
- کلمات عبور تغییر یافته برای دسترسی های بعدی باید در اختیار واحدانفورماتیک قرار گیرد.

۹ – نسخه پشتیبان

نسخه پشتیبان شامل نسخه پشتیبان بانک های اطلاعاتی و دیتاهای سازمانی و نسخه پشتیبان از تمامی سیستم عاملهای سرورها است. مسئول تهیه نسخ پیشتیبان کارشناس واحد انفور ماتیک با نظارت مدیر واحد است .

دستورالعمل:

- کلیه اطلاعات سازمانی به صورت روزانه پشتیبان تهیه شود. و این اطلاعات ۱ ماه برروی سروراقی بماند.
- سیستم عامل سرورها ۱۵روز یک بار باید نسخه پشتیبان داشته باشند و محل ذخیره سازی آنها روی سرور است.
- در حال حاضر دیتاهای سرورها با نرم افزار آکرونیس و سرور ها با Veem نسخه پشتیبان تهیه می شود.
- کلیه نسخ پشتیبان باید بر روی رسانه ذخیره سازی مورد تایید 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:

۱-نام سیستمی که از آن نسخه پشتیبان تهیه شده است.

۲-تاریخ تهیه نسخه پشتیبان

۳-میزان اهمیت اطلاعاتی که از آنها نسخه پشتیبان تهیه شده است.

۴-نام فردی که نسخه پشتیبان را تهیه کرده است.

۵-تاریخ مصرف نسخه پشتیبان

۶- برای نسخه پشتیبان رمز تعریف گردد.

۷- خارج نمون نسخ پشتیبان از سازمان بصورت ماهانه صورت گیرد .

۸-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 می شود.
- سیستم عاملهای دارای مشکل نیز روی سرورها با نرم افزار Veem برگردانده می شود.
- اطلاعات بانک اطلاعاتی نیز که روی دیسکهای بلوری ذخیره شده اند نیز با قابلیت خود نرم افزار SQL برگردانده می شوند.

۱۰- امنیت فیزیک و محیطی

۱۰-۱- دسترسی به تاسیسات اطلاعاتی

امنیت فیزیکی کلیه کامپیوتر ها و تجهیزات ارتباطی که متعلق به سازمان است و یا توسط سازمان مورد استفاده قرار می گیرند توسط تمامی کارمندان، مدیران، پیمان کاران، کارمندان پاره وقت، کارمندان موقت، کارآموزان و دیگر کارکنانی را که مجاز به دسترسی به سیستم های اطلاعاتی سازمان شناخته شده اند، باید مورد توجه قرار گیرد.

دستورالعمل:

- دسترسی فیزیکی به محدوده های کنترل شده (محدوده هایی که در آنها سیستم های اطلاعاتی یا اطلاعات حساس نگهداری می شوند، نظیر اتاق سرورها) می بایست مدیریت شده و ثبت شوند.
- تمامی محدوده های کنترل شده می بایست نشانه گذاری و برچسب زده شوند و به تناسب حساسیت و اهمیت عملکردشان مورد حفاظت فیزیکی قرار گیرند.
- دسترسی به محدوده های کنترل شده می بایست صرفا برای کارمندان و پیمانکارانی مجاز شناخته شود که مسئولیت کاری شان 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 کنترل شده می بایست آماده شود و در مواقع از کار افتادن سیستم کنترل خودکار دسترسی مورد استفاده قرار گیرد.
- کارت های دسترسی و/یا کلید ها نمی بایست به صورت اشتراکی مورد استفاده قرار گیرند و یا به دیگران قرض داده شوند.
- کارت های دسترسی و/یا کلیدهایی که دیگر مورد نیاز نیستند، می بایست به مسئول محدوده کنترل شده بازپس داده شوند. کارتها نباید بدون طی مراحل بازگرداندن، به افراد دیگر اختصاص داده شوند.
- دسترسی بازدیدکنندگان به محدوده های کنترل شده می بایست مطابق دستورالعمل بازدیدکنندگان باشد.

۱۰-۲- نواحی امن:

هدف: جلوگیری از دسترسی فیزیکی غیر مجاز، خسارت و مداخله در اطلاعات و امکانات پردازش اطلاعات

۱۰-۲-۱- حصار امنیتی فیزیکی:

دستورالعمل

- وجود یک اتاق برای نگهداری سرورها و رکها الزامی می باشد.
- کنترل دمای اتاق در دمای ۲۲ درجه سانتیگراد نگهداشته شود .
- اندسته از تجهیزاتی که در سطح سازمان بدلایل ساختار فیزیکی نصب شده اند در رک مجهز به قفل نگهداری شوند .

۱۰-۲-۲- کنترل های مداخل فیزیکی:

دستورالعمل

- کلیه مداخل فیزیکی باید مجهز به قفل و دوربین های مداربسته باشد.

۱۰-۲-۳- امن سازی دفاتر، اتاق ها و امکانات:

دستورالعمل

- باید محل های سرورها ایزوله باشد و به جز مسئولین انفورماتیک کسی اجازه دسترسی به سرورها و سوییچ ها و تجهیزات را نداشته باشد.

۱۰-۲-۴- محافظت در مورد تهدیدهای محیطی و بیرونی :

انواع تهدیدهای متعارف

مصادیق محیطی(E)	مصادیق اقدام انسان	
	تصادفی(A)	عمدی(D)
✓ زلزله ✓ گردباد ✓ رعد و برق ✓ سیل (D,A) ✓ نوسان برق (A) ✓ دما و رطوبت زیاد (D,A) ✓ گرد و غبار ✓ تخریب محیط ذخیره سازی	✓ نقص در سیستم تهویه (D) ✓ نقص در سخت افزار ✓ اشکال در تعمیرات (D) ✓ اشکال در نرم افزار (D) ✓ استفاده از نرم افزار توسط افراد غیرمجاز (D) ✓ استفاده از نرم افزار به شیوه ای غیرمجاز (D) ✓ استفاده از نرم افزار خارج از قواعد (D) ✓ نقص فنی در اجزای شبکه ✓ خطا در انتقال ✓ آسیب دیدن خطوط (D) ✓ ترافیک بیش از اندازه در شبکه (D) ✓ حذف فایل (D) ✓ نقض در خدمات ارتباطی مثال خدمات شبکه(D)	✓ اقدامات صنعتی، حمله با بمب، استفاده از سلاح، آتش افروزی(A) ✓ آسیب عمدی ✓ دزدی ✓ استفاده غیرمجاز از محیط ذخیره سازی ✓ تغییر هویت و جعل هویت ✓ نرم افزارهای مخرب(A) ✓ 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(A)

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

۱۰-۳- امنیت کابل کشی:

دستورالعمل

- کلیه کابل کشی ها باید چک شود و اگر آسیب و یا نقصی در کابل کشی هست باید توسط واحد انفورماتیک و نت تعمیر شود. این کابل کشی شامل کابل کشی شبکه و تلفن و می باشد.

۱۰-۴- خروج دارایی ها:

دستورالعمل

- تجهیزات، نرم افزارها و اطلاعات بدون مجوز قبلی نباید از شرکت خارج شوند. این محوز به عهده واحد انفورماتیک و انبار با هماهنگی مدیر مربوطه می باشد.

۱۰-۵- امنیت تجهیزات و دارایی های خارج از محوطه

امنیت تمام دارایی های درون پروژه ها بر عهده مدیر پروژه می باشد .

۱۰-۶- امحا و 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 (Format 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 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 روشهایی استفاده نمود که بازیابی توسط تکنیک های تخصصی نیز امکان پذیر نباشد.

دستورالعمل:

- 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 و یا انهدام، پاک شوند.
- اطلاعات تمامی بستر های ذخیره سازی اطلاعات سیستم ها و قطعاتی که در سازمان مجددا مورد استفاده قرار می گیرند، باید با یک نرم افزار مورد تایید پاک شوند. دربرخی از موارد باید از سیستم ها پیش از استفاده مجدد یک نسخه پشتیبان کامل تهیه شود.
- تمامی بستر های ذخیره سازی سیستم ها و تجهیزاتی که مورد استفاده مجدد قرار گرفته، فروخته شده و یا بخشیده می شوند و یا حتی به عنوان وسایل غیر قابل استفاده به بیرون از سازمان منتقل می شوند، لازم است توسط نرم افزار مورد تایید پاک شوند.
- تمامی عملیات پاک کردن و یا انهدام تجهیزات می باید با اطلاعات زیر ثبت شوند:

  - تاریخ و زمان عملیات

  - نام، عنوان و امضاء کارشناس مربوطه

  - شرح اقدامات انجام گرفته

۱۰-۷- میز پاک و صفحه پاک:

برقراری استانداردهای امنیت فیزیکی ایستگاه های کاری و برای پیشگیری از سرقت ایستگاه های کاری تمامی کارمندان، مدیران، پیمان کاران، کارمندان پاره وقت، کارمندان موقت و دیگر کارکنانی را که مجاز به دسترسی به سیستم های اطلاعاتی سازمان شناخته شده انداین ضروری است.

دستورالعمل:

- کاربران ایستگاه های کاری نباید هیچ دستگاه جانبی که فاقد تاییدیه واحد انفورماتیک است را به ایستگاه های کاری متصل کنند.
- مانیتورهای ایستگاه های کاری می بایست به گونه ای قرار گیرند که از دیده شدن اطلاعات حساس توسط افراد غیر مجاز جلوگیری شود.

- کاربران در هنگام ترک ایستگاه کاری می بایست شخصا از ایستگاه خارج شوند (Logoff کنند) و ایستگاه ها می بایست به صورت خودکار در صورت عدم فعالیت کاربر، قفل شوند (Lock) و یا از محیط خارج شوند (Log off).
- ایستگاه های کاری قابل حمل، در زمانهایی که بدون متصدی رها می شوند، صرف نظر از اقدامات امنیتی ساختمان، می بایست به صورت فیزیکی محافظت شوند. این محافظت می تواند به روش قرار دادن در میز ها یا کمدهای دارای قفل باشد
- در هنگام سفر، ایستگاه های کاری قابل حمل در هیچ زمان نمی بایست بدون متصدی رها شوند. وقتی که در محیط کار اصلی، محیط کار امن نمی باشند تجهیزات قابل حمل نمی بایست از کارمند جدا شود. این موضوع بخصوص در فرودگاه، اتومبیل، اتاق هتل و رستوران می بایست مورد توجه قرار گیرد.
- ایستگاه های کاری به سرقت رفته و یا مفقود شده، یک رخنه امنیتی را به وجود می آورند و باید سریعاً به واحد انفورماتیک گزارش شوند.