



روش اجرایی مدیریت و ساماندهی فایل‌های الکترونیکی و
تجهیزات فناوری اطلاعات در چارچوب نظام آراستگی (5S)
در اتاق بازرگانی، صنایع، معادن و کشاورزی اصفهان

ECCIM.COM

نام مدرک	روش اجرایی مدیریت و ساماندهی فایل های الکترونیکی و تجهیزات فناوری اطلاعات در چارچوب نظام آراستگی (5S) در اتاق بازرگانی، صنایع، معادن و کشاورزی اصفهان
کد مدرک	SY-PR-17-00-01
تاریخ ایجاد مدرک	۱۴۰۵/۰۶/۲۱
شماره بازنگری	۰۱
تاریخ آخرین بازنگری	۱۴۰۵/۰۶/۲۱
تعداد صفحات	۱۵
سطح امنیت	عمومی
دسترسی	کلیه واحدها و کارکنان در اتاق بازرگانی، صنایع، معادن و کشاورزی اصفهان

شماره بازنگری	موضوع و ماهیت تغییر

امضا	تاریخ	سمت	نام	
		مدیر برنامه ریزی استراتژیک و تحول سازمانی	پدرام برومند	تهیه کننده
		مدیر برنامه ریزی استراتژیک و تحول سازمانی	پدرام برومند	تأیید کننده
		دبیر کل	حمیدرضا امیدان	تصویب کننده

محل مهر



فهرست

۱.....	فصل اول.....
۱-۱.....	هدف (Purpose).....
۱-۲.....	دامنه کاربرد (Scope).....
۱-۳.....	ذی نفعان (Stakeholders).....
۱-۴.....	تعاریف و واژگان.....
۱-۴-۱.....	اتفاق.....
۱-۴-۲.....	رکورد الکترونیکی.....
۱-۴-۳.....	اطلاعات الکترونیکی.....
۱-۴-۴.....	نسخه پشتیبان.....
۱-۴-۵.....	اطلاعات قابل اعتماد.....
۱-۴-۶.....	بایگانی جاری.....
۱-۴-۷.....	امحاء اطلاعات.....
۲.....	فصل دوم: اقدامات.....
۲-۱.....	محل های مجاز ذخیره سازی اطلاعات.....
۲-۱-۱.....	ممنوعیت های ذخیره سازی اطلاعات.....
۲-۲.....	طبقه بندی فایل ها بر اساس ضرورت نگهداری.....
۲-۳.....	ساختار استاندارد پوشه بندی.....
۲-۴.....	نام گذاری فایل ها.....
۲-۵.....	طبقه بندی امنیتی اطلاعات.....
۲-۶.....	آرشیو فایل های الکترونیکی.....
۲-۶-۱.....	معیارهای انتقال اطلاعات به آرشیو.....
۲-۶-۲.....	فرآیند آرشیو.....
۲-۶-۳.....	الزامات محل نگهداری آرشیو.....
۲-۷.....	دوره های نگهداری اطلاعات.....
۲-۸.....	امحاء اطلاعات.....



۱۴۰۵/۰۶/۲۱

- ۸-۲-۱. ثبت سوابق امحاء..... ۱۰
- ۹-۲-۱. پشتیبان گیری و بازیابی اطلاعات..... ۱۰
- ۹-۲-۱. دامنه پشتیبان گیری..... ۱۰
- ۹-۲-۲. سیاست پشتیبان گیری..... ۱۱
- ۹-۲-۳. محل نگهداری نسخه های پشتیبان..... ۱۱
- ۹-۲-۴. کنترل و آزمون بازیابی اطلاعات..... ۱۲
- ۹-۲-۵. امنیت نسخه های پشتیبان..... ۱۲
- ۱۰-۲-۱. الزامات ساماندهی و نگهداری تجهیزات و زیرساخت فناوری اطلاعات (IT)..... ۱۳
- ۱۰-۲-۱-۱. مدیریت و ساماندهی کابل ها و سیم کشی..... ۱۳
- ۱۰-۲-۲. تفکیک و مسیر گذاری کابل ها..... ۱۳
- ۱۰-۲-۳. استقرار تجهیزات فناوری اطلاعات..... ۱۳
- ۱۰-۲-۴. مدیریت تجهیزات جانبی و اقلام مصرفی..... ۱۴
- ۱۰-۲-۵. الزامات اختصاصی اتاق سرور و تجهیزات شبکه..... ۱۴
- ۱۱-۲-۱۱. پیوست..... ۱۵



۱. فصل اول

۱-۱. هدف (Purpose)

این مستند با هدف استقرار نظام یکپارچه مدیریت و ساماندهی فایل‌های الکترونیکی، ارتقای نظم و آراستگی دیجیتال^۱، حفاظت از دارایی‌های اطلاعاتی سازمان و تضمین دسترسی، بازیابی و ردیابی اطلاعات تدوین شده است. همچنین، ساماندهی، نگهداری و بهره‌برداری مناسب از تجهیزات و زیرساخت‌های فناوری اطلاعات (IT) در چارچوب نظام آراستگی سازمان مورد توجه قرار می‌گیرد. اهداف اصلی این مستند عبارت‌اند از:

- ایجاد رویه‌ای یکپارچه و استاندارد برای ذخیره‌سازی، نام‌گذاری، طبقه‌بندی و مدیریت فایل‌های الکترونیکی در سطح سازمان.
- تضمین اصالت، یکپارچگی، محرمانگی و دسترس‌پذیری اطلاعات.
- ساماندهی، طبقه‌بندی و مدیریت آرشیو دیجیتال سازمان.
- تعیین ضوابط مربوط به پشتیبان‌گیری، نگهداری و بازیابی اطلاعات.
- فراهم‌سازی امکان ممیزی، ردیابی و اثبات‌پذیری سوابق الکترونیکی.
- کاهش ریسک حذف، مفقودی، خرابی یا دسترسی غیرمجاز به اطلاعات و اطمینان از وجود نسخه‌های پشتیبان معتبر
- ساماندهی، نگهداری مربوط به تجهیزات و زیرساخت‌های فناوری اطلاعات در محیط‌های سازمانی.
- حمایت از استقرار، تداوم و بهبود نظام آراستگی (5S) در محیط فیزیکی و دیجیتال سازمان.

۱-۲. دامنه کاربرد (Scope)

این مستند در خصوص کلیه اطلاعات، اسناد و فایل‌های الکترونیکی ایجاد، دریافت، پردازش، ذخیره‌سازی یا نگهداری شده در سازمان، خارج از دامنه شمول روش اجرایی کنترل سوابق، مدارک و مستندات سیستم مدیریت کیفیت به شماره مستند (SY-PR-04) و همچنین زیرساخت‌ها و سامانه‌های فناوری اطلاعات مورد استفاده در پشتیبانی از اطلاعات اتاق بازرگانی، صنایع، معادن و کشاورزی اصفهان کاربرد دارد.

این مستند کلیه واحدها و کارکنانی را که در ایجاد، استفاده، نگهداری، مدیریت یا دسترسی به این منابع نقش دارند، دربرمی‌گیرد. دامنه کاربرد این مستند شامل موارد زیر است:

¹ Digital 5S



- سرورها و تجهیزات و سامانه‌های ذخیره‌سازی تحت شبکه شامل File Server، NAS و SAN.
- سامانه‌ها و نرم‌افزارهای کاربردی سازمانی شامل سامانه‌های مالی، عضویت، مکاتبات و اتوماسیون اداری، ERP و سایر نرم‌افزارهای تخصصی.
- فایل‌ها، اسناد و مستندات الکترونیکی ایجاد شده، دریافت شده یا مورد استفاده واحدهای سازمانی.
- آرشیوهای دیجیتال، مخازن اطلاعاتی و پوشه‌های اشتراکی سازمان.
- نسخه‌های پشتیبان اطلاعات و داده‌های سازمانی (Backup).
- فایل‌های چندرسانه‌ای شامل تصاویر، ویدئوها و فایل‌های صوتی سازمانی.
- سایر تجهیزات و زیرساخت‌های فناوری اطلاعات مرتبط با ذخیره‌سازی، پردازش، انتقال، نگهداری و دسترسی به اطلاعات سازمان.

۳-۱. ذی‌نفعان (Stakeholders)

- دبیر کل: مسئولیت تصویب و ابلاغ این روش اجرایی را بر عهده دارد.
- واحد سیستم‌ها و روش‌ها: مسئولیت تهیه، تدوین، تأیید و به‌روزرسانی روش اجرایی را بر عهده دارد و همچنین نظارت بر حسن اجرای این روش اجرایی بر عهده این واحد است.
- کلیه واحدها: مسئولیت اجرای این روش اجرایی را بر عهده دارد.

۴-۱. تعاریف و واژگان

۱-۴-۱. اتاق

منظور از اتاق در این مستند، اتاق بازرگانی، صنایع، معادن و کشاورزی اصفهان است.

۲-۴-۱. رکورد الکترونیکی^۲

هرگونه داده، اطلاعات، فایل یا سند الکترونیکی که در نتیجه فعالیت‌های سازمان ایجاد یا دریافت شده و به‌عنوان مدرک یا سابقه رسمی و قابل استناد سازمان نگهداری می‌شود.

۳-۴-۱. اطلاعات الکترونیکی^۳

کلیه داده‌ها و اطلاعات ایجاد، دریافت، پردازش، ذخیره یا منتقل شده در قالب الکترونیکی، از جمله اسناد و فایل‌های متنی، ایمیل‌ها، پایگاه‌های داده، تصاویر، فایل‌های صوتی و ویدئویی.

^۲ Electronic Record

^۳ Electronic Information



۱۴۰۵/۰۶/۲۱

۴-۴-۱. نسخه پشتیبان^۴

نسخه ای از داده ها و اطلاعات که با هدف امکان بازیابی آن ها در صورت بروز خرابی، حذف، از دست رفتن اطلاعات، حمله سایبری یا سایر شرایط بحرانی، تهیه و در محل یا بستر مناسب نگهداری می شود.

۵-۴-۱. اطلاعات قابل اعتماد^۵

اطلاعاتی که اصالت، صحت، یکپارچگی و قابلیت دسترس پذیری آن در طول دوره نگهداری، و تایید دبیرکل باشد.

۶-۴-۱. بایگانی جاری

فضای فیزیکی یا الکترونیکی اختصاص یافته به نگهداری اطلاعات و اسنادی که در فرآیندهای عملیاتی روزمره مورد استفاده قرار می گیرند.

۷-۴-۱. امحاء اطلاعات

فرآیند حذف یا نابودی ایمن اطلاعات به گونه ای که پس از پایان دوره نگهداری مصوب، امکان بازیابی یا دسترسی مجدد به اطلاعات وجود نداشته باشد.

⁴ Backup⁵ Trustworthy Information



۲. فصل دوم: اقدامات

۲-۱. محل‌های مجاز ذخیره‌سازی اطلاعات

کلیه فایل‌ها، اسناد و اطلاعات سازمانی باید صرفاً در محل‌ها و بسترهای ذخیره‌سازی تعیین شده توسط واحد فناوری اطلاعات و زیرساخت ذخیره و نگهداری شوند. کاربران موظف‌اند متناسب با نوع و وضعیت اطلاعات، محل مناسب ذخیره‌سازی را انتخاب نموده و از ایجاد نسخه‌های غیرضروری و پراکنده اطلاعات خودداری نمایند. محل‌های مجاز ذخیره‌سازی اطلاعات عبارت‌اند از:

الف) فضای صفحه نمایشگر^۶

جهت نگهداری موقت فایل‌های در حال پردازش و فایل‌های مورد استفاده روزانه کاربران که به دسترسی سریع نیاز دارند. نگهداری بلندمدت یا آرشیو اطلاعات سازمانی در این فضا مجاز نیست.

ب) فضای ذخیره^۷

جهت نگهداری مستندات جاری، سوابق کاری و اطلاعات سازمانی که نیازمند حفاظت، نگهداری مستمر و دسترسی کنترل شده هستند. اطلاعاتی که باید به‌عنوان سابقه یا مرجع سازمانی نگهداری شوند، باید در این فضا ذخیره شوند.

ج) فضای اشتراک فایل^۸

جهت تبادل و اشتراک‌گذاری موقت فایل‌ها بین کاربران و واحدهای سازمانی استفاده می‌شود.

تبصره: کلیه اطلاعات موجود در فضای Share باید به‌صورت ماهانه توسط واحد فناوری اطلاعات و زیرساخت مورد پایش قرار گیرد. در این راستا، واحد مذکور موظف است از طریق نامه داخلی، واحدهای مربوطه را ملزم نماید نسبت به بازبینی و پاکسازی اطلاعات مازاد خود اقدام کنند.

نگهداری اطلاعات دائمی، سوابق رسمی و فایل‌های موردنیاز برای نگهداری بلندمدت در فضای Share مجاز نیست و کاربران موظف‌اند اطلاعات موردنیاز را پیش از انجام پاکسازی، به محل ذخیره‌سازی مناسب منتقل نمایند. در صورت عدم انتقال یا تعیین تکلیف اطلاعات توسط واحد مربوطه، واحد فناوری اطلاعات و زیرساخت مجاز است با هماهنگی و تأیید دبیر کل نسبت به بازبینی و پاکسازی اطلاعات موجود در فضای Share اقدام نماید.

^۶ Desktop

^۷ Storage

^۸ Share





۱-۱-۲. ممنوعیت های ذخیره سازی اطلاعات

موارد زیر ممنوع است:

- ذخیره فایل ها و اطلاعات سازمانی در حافظه ها و تجهیزات شخصی، از جمله حافظه های قابل حمل، بدون مجوز واحد فناوری اطلاعات و زیرساخت.
- نگهداری فایل ها و اطلاعات سازمانی در رایانه ها یا تجهیزات شخصی خارج از زیرساخت فناوری اطلاعات اتاق.
- ایجاد پوشه ها، مسیرها و ساختارهای ذخیره سازی خارج از چارچوب و ساختار مصوب.
- نگهداری بلندمدت اطلاعات سازمانی در فضای Desktop یا Share.
- ایجاد نسخه های متعدد و غیرضروری از یک فایل در محل های مختلف ذخیره سازی.
- انتقال یا ذخیره اطلاعات سازمانی در سرویس های ذخیره سازی ابری یا سامانه های خارج از سازمان، بدون مجوز واحد فناوری اطلاعات و زیرساخت.

۲-۲. طبقه بندی فایل ها بر اساس ضرورت نگهداری

فایل های ضروری شامل فایل هایی هستند که:

- در فرآیندهای جاری سازمان مورد استفاده قرار می گیرند.
- به عنوان مرجع رسمی سازمان شناخته می شوند.
- فایل های غیرضروری شامل فایل هایی هستند که:
- فاقد استفاده مشخص هستند.
- تکراری یا زائد هستند.
- منسوخ شده اند.
- فاقد مالک مشخص هستند.
- فاقد ارزش عملیاتی یا قانونی هستند.

در صورت نیاز به نگهداری طولانی مدت فایل ها، مدیر واحد مربوطه درخواست آرشیو فایل ها را به واحد فناوری اطلاعات و زیرساخت اعلام می نماید. واحد فناوری اطلاعات و زیرساخت پس از بررسی درخواست، موضوع را جهت هماهنگی و اخذ تأیید دبیرکل پیگیری نموده و پس از تأیید، نسبت به آرشیو فایل ها و تهیه نسخه پشتیبان اقدام می نماید. پس از اطمینان از ثبت و نگهداری صحیح فایل ها در آرشیو و تهیه نسخه پشتیبان، نسخه موجود در محیط کاربری حذف می گردد.



جدول ۱- جدول طبقه بندی فایل ها و نگهداری آن ها

ردیف	طبقه فایل	شرح	نمونه ها	محل نگهداری	دوره نگهداری
۱	فایل های عملیاتی جاری	فایل هایی که به طور مستمر در فعالیت های روزانه و فرآیندهای جاری مورد استفاده قرار می گیرند.	مکاتبات جاری، گزارش های در حال تهیه، فرم های فعال، پروژه های جاری	پوشه های عملیاتی واحد	تا پایان فرآیند یا فعالیت
۲	فایل های مرجع و سازمانی	فایل هایی که به عنوان مرجع رسمی و معتبر سازمان مورد استفاده قرار می گیرند.	دستورالعمل ها، آیین نامه ها، روش های اجرایی، فرم های مصوب	روش اجرایی کنترل سوابق مدارک و مستندات سیستم مدیریت کیفیت به شماره مستند (SY-PR-04)	تا زمان اعتبار یا جایگزینی با نسخه جدید
۳	فایل های آرشیوی	اطلاعاتی که نگهداری آن ها بر اساس قوانین، مقررات و تایید دبیر کل است.	اسناد مالی، قراردادها، سوابق پرسنلی، پرونده های حقوقی	آرشیو الکترونیکی	براساس تایید دبیر کل
۴	فایل های آرشیوی	فایل هایی که استفاده روزمره ندارند، اما نگهداری آن ها به منظور حفظ سوابق سازمانی ضروری است.	گزارش های سنواتی، مستندات پروژه های خاتمه یافته، صورت جلسات	فضای آرشیو دیجیتال	براساس تایید دبیر کل
۵	فایل های موقت	فایل هایی که با هدف تبادل اطلاعات یا انجام فعالیت های کوتاه مدت ایجاد یا دریافت می شوند و پس از اتمام فعالیت ارزش نگهداری ندارند.	فایل های تبادلی، نسخه های موقت، فایل های کاری بین واحدی	فضای اشتراکی یا پوشه موقت	حداکثر ۷ روز
۶	فایل های تکراری	نسخه های اضافی و غیر ضروری از فایل های اصلی که ارزش مستقل برای نگهداری ندارند.	کپی های متعدد یک سند، فایل های دابلود شده تکراری	حذف یا ادغام با نسخه اصلی	پس از شناسایی و بررسی
۷	فایل های منسوخ	فایل هایی که اعتبار یا کاربرد جاری خود را از دست داده اند، اما به منظور سوابق سازمانی یا تأیید دبیر کل نیاز به نگهداری دارند.	نسخه های قدیمی دستورالعمل ها، فرم های ابطال شده	آرشیو منسوخ	براساس تایید دبیر کل
۸	فایل های فاقد ارزش نگهداری	فایل هایی که فاقد ارزش عملیاتی، قانونی، قراردادی یا تاریخی بوده و نیازی به نگهداری ندارند.	فایل های آزمایشی، پیش نویس های بلااستفاده، فایل های بدون مالک یا کاربرد مشخص	حذف ایمن	حداکثر ۳۰ روز پس از شناسایی



۲-۳. ساختار استاندارد پوشه بندی

ساختار ذخیره سازی اطلاعات باید مطابق الگوی زیر باشد:

نام واحد سازمانی / سال / نوع مدرک / ماه / نام فایل

ایجاد پوشه خارج از ساختار مصوب مجاز نیست. هر سال مالی یا تقویمی نیز باید در پوشه ای مستقل نگهداری شود.

۲-۴. نام گذاری فایل ها

نام فایل ها باید به گونه ای تعیین شود که امکان جست و جو، شناسایی، بازیابی، کنترل نسخه و جلوگیری از ایجاد فایل های تکراری را فراهم نماید. فرمت استاندارد نام گذاری فایل:

YYYY/MM/DD-Subject

نمونه:

۱۴۰۵۰۳۱۳-گزارش_رویداد_عصر_آموزش

برای فایل های قابل ویرایش، از قبیل Word و Excel، درج شماره نسخه در انتهای نام فایل الزامی است.
نمونه:

۱۴۰۵۰۳۱۳-بودجه_سالانه-V01.docx

۱۴۰۵۰۳۱۳-گزارش_عملکرد-V03.xlsx

پس از نهایی شدن سند، نسخه نهایی باید با عبارت Final مشخص شود.
نمونه:

۱۴۰۵۰۳۱۳-گزارش_عملکرد-Final.pdf

تبصره: نحوه نگارش مستندات سازمان می بایست مطابق با روش اجرایی کنترل و نگارش مستندات سیستم مدیریت یکپارچه به شماره مستند (SY-PR-02) باشد.

۲-۵. طبقه بندی امنیتی اطلاعات

کلیه فایل ها و مستندات الکترونیکی مطابق با روش اجرایی کنترل و نگارش مستندات سیستم مدیریت یکپارچه به شماره مستند (SY-PR-02)، بر اساس سطح حساسیت و اهمیت اطلاعات و بنابر صلاح دید دبیر کل، در یکی از طبقات زیر طبقه بندی شوند:



- عمومی.
- محدود.
- محرمانه.

مدیریت فناوری اطلاعات و زیرساخت موظف است با هماهنگی و تأیید دبیرکل، دسترسی کاربران به اطلاعات را متناسب با سطح طبقه بندی آن ها تعریف، کنترل و پایش نماید.

۶-۲. آرشیو فایل های الکترونیکی

۶-۲-۱. معیارهای انتقال اطلاعات به آرشیو

اطلاعات و مستندات الکترونیکی در صورت احراز یک یا چند مورد از شرایط زیر، باید از فضای عملیاتی به آرشیو دیجیتال منتقل شوند:

- فرآیند یا فعالیت مرتبط با اطلاعات خاتمه یافته باشد.
- استفاده روزمره و عملیاتی از اطلاعات متوقف شده باشد.
- دوره نگهداری اطلاعات در بایگانی جاری به پایان رسیده باشد.

۶-۲-۲. فرآیند آرشیو

انتقال اطلاعات به آرشیو باید مطابق مراحل زیر انجام شود:

- ثبت درخواست: واحد مالک اطلاعات، درخواست انتقال اطلاعات به آرشیو را ثبت می نماید.
- بررسی دوره نگهداری: بنا بر تشخیص دبیرکل، کارشناس مرکز آمار و مستندسازی دوره نگهداری اطلاعات را بررسی و تأیید می نماید.
- انتقال به آرشیو: مدیریت فناوری اطلاعات و زیرساخت، پس از تأیید دوره نگهداری، نسبت به انتقال اطلاعات به فضای آرشیو اقدام می نماید.
- ثبت اطلاعات توصیفی: اطلاعات توصیفی^۹ مربوط به فایل یا پرونده، توسط کارشناس مرکز آمار و مستندسازی ثبت و نگهداری می شود.

حداقل اطلاعات مورد نیاز برای ثبت Metadata شامل موارد زیر است:

- عنوان فایل یا پرونده.

^۹ Metadata





- تاریخ انتقال به آرشیو.
- واحد یا شخص مالک اطلاعات.
- دوره نگهداری مصوب.
- تاریخ تعیین شده برای امحاء.
- سطح طبقه‌بندی امنیتی.
- محل نگهداری آرشیو.

۲-۶-۳. الزامات محل نگهداری آرشیو

فضای آرشیو دیجیتال باید، متناسب با سطح حساسیت اطلاعات، دارای ویژگی‌های زیر باشد:

- تفکیک فیزیکی یا منطقی از فضای عملیاتی سازمان.
- محدودیت دسترسی صرفاً برای افراد مجاز.
- قابلیت ثبت و پایش سوابق دسترسی.
- برخورداری از نسخه پشتیبان مستقل.
- حفاظت در برابر حذف، تغییر یا دسترسی غیرمجاز.
- استفاده از سازوکارهای رمزنگاری برای اطلاعات حساس، حسب نیاز.

۲-۷. دوره‌های نگهداری اطلاعات

دوره نگهداری اطلاعات با توجه به نیازهای سازمانی و ارزش اطلاعات، با هماهنگی واحد مالک اطلاعات و پس از تأیید دبیر کل، توسط مدیریت فناوری اطلاعات و زیرساخت و کارشناس مرکز آمار و مستندسازی تعیین می‌شود. در صورت نبود الزام قانونی یا قراردادی مشخص، دوره نگهداری اطلاعات باید مطابق با روش اجرایی کنترل سوابق مدارک و مستندات سیستم مدیریت کیفیت به شماره مستند (SY-PR-04) تعیین و ثبت گردد.

۲-۸. امحاء اطلاعات

پس از پایان دوره نگهداری مصوب، اطلاعات باید پس از بررسی و تأیید واحد مالک و مرجع ذی‌صلاح، مطابق فرآیند کنترل شده و با رعایت الزامات امنیتی امحاء شوند.

فرآیند امحاء شامل مراحل زیر است:

- بررسی و تأیید پایان دوره نگهداری توسط مسئول بایگانی یا مرجع ذی‌صلاح.
- تأیید واحد مالک اطلاعات.





۱۴۰۵/۰۶/۲۱

- اجرای حذف یا امحاء ایمن پس از تایید دبیرکل توسط مدیریت فناوری اطلاعات و زیرساخت و، در صورت لزوم، کمیته ضایعات.
- ثبت و نگهداری سوابق امحاء.

۲-۸-۱. ثبت سوابق امحاء

گزارش امحاء اطلاعات باید حداقل شامل موارد زیر باشد:

- نام فایل، پوشه یا مجموعه اطلاعات.
- مسیر ذخیره‌سازی.
- تاریخ امحاء.
- واحد مالک اطلاعات.
- مسئول اجرای امحاء.
- روش حذف یا امحاء.
- شماره مجوز یا تأییدیه امحاء.

سوابق امحاء باید مطابق ضوابط مدیریت سوابق سازمان ثبت و نگهداری شوند.

۲-۹. پشتیبان‌گیری و بازیابی اطلاعات

به منظور حفاظت از اطلاعات سازمان، کاهش ریسک از دست رفتن داده‌ها، تضمین تداوم فعالیت‌ها و فراهم‌سازی امکان بازیابی اطلاعات در شرایط خرابی، حذف، اختلال یا سایر شرایط بحرانی، مدیر فناوری اطلاعات و زیرساخت پس از تایید دبیرکل موظف است فرآیند پشتیبان‌گیری و بازیابی اطلاعات را مطابق ضوابط این مستند اجرا، کنترل و پایش نماید.

۲-۹-۱. دامنه پشتیبان‌گیری

پشتیبان‌گیری از اطلاعات و زیرساخت‌های سازمان، متناسب با اهمیت و حساسیت اطلاعات، باید حداقل شامل موارد

زیر باشد:

- فایل سرورها و مخازن اطلاعاتی.
- پایگاه‌های داده^{۱۰}.
- سامانه‌های کاربردی و نرم‌افزارهای سازمانی.

¹⁰ Databases



- تنظیمات و پیکربندی سرورها و تجهیزات مرتبط.
- لاگ های سیستمی و امنیتی، حسب نیاز سازمان.
- آرشیوهای دیجیتال سازمان.

۲-۹-۲. سیاست پشتیبان گیری

پشتیبان گیری از اطلاعات مطابق برنامه جدول ۲ انجام می شود:

جدول ۲- برنامه پشتیبان گیری اطلاعات

مدت نگهداری	تناوب اجرا	نوع پشتیبان گیری
سه ماه	هفتگی	پشتیبان گیری کامل ^{۱۱}
۳۰ روز	روزانه	پشتیبان گیری افزایشی ^{۱۲}
یکسال	ماهانه	پشتیبان گیری آرشیوی

تبصره: بنابر صلاح دید دبیر کل و تشخیص مدیر فناوری اطلاعات و زیرساخت و کارشناس مرکز آمار و مستندسازی، قراردادی یا سازمانی، دوره های نگهداری اطلاعات و نسخه های پشتیبان می تواند افزایش یابد.

تبصره: تناوب و روش پشتیبان گیری از سامانه ها و اطلاعات حساس، متناسب با اهمیت اطلاعات، میزان تغییرات و نیازهای عملیاتی سازمان، می تواند با تأیید دبیر کل و مدیر فناوری اطلاعات و زیرساخت افزایش یا بازنگری شود.

تبصره: مدیر فناوری اطلاعات و زیرساخت موظف است به صورت دوره ای قابلیت بازیابی نسخه های پشتیبان را آزمون و از صحت و قابلیت استفاده از آن ها اطمینان حاصل نماید.

۲-۹-۳. محل نگهداری نسخه های پشتیبان

به منظور کاهش ریسک از دست رفتن اطلاعات و افزایش قابلیت بازیابی در شرایط بحرانی، نسخه های پشتیبان اطلاعات

باید حداقل در دو محل مستقل و مجزا نگهداری شوند:

- یک نسخه در محل سازمان^{۱۳}.
- یک نسخه در محل مستقل و خارج از سازمان^{۱۴}.

¹¹ Full Backup
¹² Incremental Backup
¹³ On-Site
¹⁴ Off-Site

در صورت فراهم بودن زیرساخت های مورد تأیید سازمان و رعایت الزامات امنیتی، نگهداری نسخه رمزنگاری شده اطلاعات در فضای ابری سازمانی نیز مجاز است.

تبصره: محل نگهداری نسخه های پشتیبان باید به گونه ای انتخاب شود که در صورت وقوع حوادثی مانند آتش سوزی، سرقت، خرابی تجهیزات یا سایر حوادث مؤثر بر محل اصلی، امکان دسترسی به نسخه پشتیبان و بازیابی اطلاعات وجود داشته باشد.

۲-۹-۴. کنترل و آزمون بازیابی اطلاعات

به منظور اطمینان از صحت، کامل بودن و قابلیت استفاده از نسخه های پشتیبان، آزمون بازیابی اطلاعات باید حداقل هر شش ماه یکبار انجام شود. بازیابی ها عبارت اند از:

- بازیابی نمونه ای از فایل ها و اطلاعات منتخب.
 - بازیابی پایگاه های داده یا سامانه های حیاتی، متناسب با امکان و شرایط فنی.
 - بررسی صحت، کامل بودن و قابلیت استفاده از اطلاعات بازیابی شده.
 - شناسایی و ثبت خطاها، مغایرت ها و مشکلات احتمالی.
 - ثبت نتایج آزمون و اقدامات اصلاحی مورد نیاز.
- گزارش نتایج آزمون بازیابی، شامل تاریخ آزمون، اطلاعات یا سامانه های مورد آزمون، نتیجه بازیابی، مشکلات شناسایی شده و اقدامات اصلاحی انجام شده، پس از تایید دبیرکل توسط مدیر فناوری اطلاعات و زیرساخت ثبت و نگهداری شود.

۲-۹-۵. امنیت نسخه های پشتیبان

به منظور حفظ محرمانگی، یکپارچگی و دسترس پذیری نسخه های پشتیبان و جلوگیری از دسترسی، تغییر، افشا یا حذف غیر مجاز آنها، رعایت موارد زیر الزامی است:

- دسترسی به نسخه های پشتیبان صرفاً برای افراد مجاز و متناسب با سطح دسترسی تعیین شده مجاز است.
- کلیه عملیات مرتبط با دسترسی، بازیابی، انتقال، تغییر و حذف نسخه های پشتیبان، حسب قابلیت فنی سامانه، باید در لاگ های سیستمی ثبت و قابل ردیابی باشد.
- از تغییر، حذف، جایگزینی یا دستکاری غیر مجاز نسخه های پشتیبان باید جلوگیری شود.
- سطوح دسترسی و مجوزهای مرتبط با نسخه های پشتیبان باید به صورت دوره ای بازبینی و در صورت تغییر مسئولیت یا سطح دسترسی افراد، اصلاح یا لغو شوند.

- نسخه های پشتیبان باید در برابر بدافزار، باج افزار و سایر تهدیدات امنیتی، متناسب با سطح ریسک و اهمیت اطلاعات، محافظت شوند.

۱-۲. الزامات ساماندهی و نگهداری تجهیزات و زیرساخت فناوری اطلاعات (IT)

۱-۱۰-۲. مدیریت و ساماندهی کابل ها و سیم کشی

- کلیه کابل های برق، شبکه، تلفن، تصویر و سایر کابل های ارتباطی باید در هر دو سر دارای برچسب شناسایی باشند. برچسب ها حداقل باید شامل نوع کابل، مبدأ، مقصد و کد تجهیز مرتبط باشند.
- کابل ها باید به صورت منظم در داکت، ترانکینگ، سینی کابل یا سایر تجهیزات استاندارد مدیریت کابل قرار گرفته و از رهاسازی آن ها بر روی کف یا محیط کار جلوگیری شود.
- طول اضافی کابل ها باید جمع آوری و با استفاده از بست های استاندارد مدیریت کابل^{۱۵} مهار شوند.
- استفاده از روش های غیر استاندارد، از جمله چسب نواری، برای بستن یا جمع آوری کابل ها ممنوع است.
- کابل های بلااستفاده، فرسوده یا فاقد کاربرد باید شناسایی و برچسب گذاری شده و جهت تعیین تکلیف دارایی ها، جمع آوری و از مدار استفاده خارج شوند.

۲-۱۰-۲. تفکیک و مسیر گذاری کابل ها

- مسیر عبور کابل های برق، شبکه، تلفن، سیستم های حفاظتی و تجهیزات صوتی و تصویری باید تا حد امکان به صورت مجزا و قابل شناسایی طراحی و اجرا شود.
- به منظور کاهش نویز و اختلالات الکترومغناطیسی، مسیر کابل های برق باید حتی الامکان از مسیر کابل های شبکه و مخابراتی تفکیک شود.
- کلیه مسیرهای کابل کشی باید دارای نظم، قابلیت ردیابی و دسترسی مناسب برای انجام تعمیرات و عملیات نگهداری باشند.

۳-۱۰-۲. استقرار تجهیزات فناوری اطلاعات

- کلیه تجهیزات زیرساختی شامل مودم، روتر، سوئیچ، سرور، UPS و سایر تجهیزات ارتباطی باید در محل های تعیین شده و مطابق الزامات ایمنی و فنی نصب و مستقر شوند.
- استقرار تجهیزات فناوری اطلاعات به صورت مستقیم بر روی زمین ممنوع است و تجهیزات باید در رک، قفسه، استند یا سایر تجهیزات مناسب قرار گیرند.



- در صورت استفاده از رک، کلیه تجهیزات نصب شده باید دارای شماره شناسایی و موقعیت مشخص در نقشه رک^{۱۶} باشند.

- دسترسی به تجهیزات فناوری اطلاعات نباید توسط تجهیزات، اسناد، اقلام اضافی یا سایر موانع مسدود شود.

۲-۱۰-۴. مدیریت تجهیزات جانبی و اقلام مصرفی

- برای نگهداری تجهیزات جانبی شامل ماوس، صفحه کلید، آداپتور، شارژر، کابل های یدکی، حافظه های جانبی و سایر اقلام مرتبط، باید محل مشخص، مناسب و دارای برچسب تعیین شود.
- تجهیزات جانبی بلااستفاده، معیوب یا مازاد باید مطابق فرآیند تعیین تکلیف دارایی ها، شناسایی، جمع آوری و ساماندهی شوند.
- موجودی تجهیزات یدکی و اقلام مصرفی فناوری اطلاعات باید به صورت دوره ای کنترل و ثبت شود.

الزامات ایمنی

- عبور یا رهاسازی کابل ها در مسیرهای تردد کارکنان و مراجعان ممنوع است.
- استفاده از چندراهی های غیراستاندارد یا اتصال زنجیره ای چندراهی ها ممنوع است.
- وضعیت فیزیکی کابل ها، اتصالات، پریزها و تجهیزات برقی باید به صورت دوره ای بازبینی شده و موارد معیوب در اسرع وقت اصلاح یا تعویض شوند.
- کلیه تجهیزات برقی و فناوری اطلاعات باید مطابق الزامات ایمنی و مستندهای سازنده مورد بهره برداری قرار گیرند.

- در صورت مشاهده هرگونه آسیب، پارگی، اتصالی، داغ شدن غیرعادی یا سایر علائم خطر در تجهیزات و کابل ها، موضوع باید فوراً به واحد فناوری اطلاعات گزارش شود.

۲-۱۰-۵. الزامات اختصاصی اتاق سرور و تجهیزات شبکه

- نگهداری هرگونه وسیله غیرمرتبط، از قبیل پرونده ها، اسناد، کارتن، تجهیزات اداری و اقلام شخصی، در اتاق سرور ممنوع است.
- کف اتاق سرور و فضای پیرامون تجهیزات باید همواره عاری از کابل های پراکنده، اقلام اضافی و موانع فیزیکی باشد.

¹⁶ Rack Layout





۱۴۰۵/۰۶/۲۱

- تجهیزات موجود در اتاق سرور و رک ها باید دارای شناسه مشخص بوده و اطلاعات مربوط به محل استقرار و مشخصات آن ها در مستندات مربوطه ثبت و به روز نگهداری شود.
- نقشه شبکه، نقشه کابل کشی، نقشه رک، فهرست تجهیزات و سایر مستندات مرتبط باید به روز بوده و در محل یا سامانه تعیین شده نگهداری شوند.
- نظافت، ساماندهی و وضعیت تجهیزات اتاق سرور و شبکه باید به صورت دوره ای و در چارچوب برنامه های بازدید و ممیزی نظام آراستگی (5S) مورد ارزیابی قرار گیرد.

۱۱-۲. پیوست

SY-PR-04	روش اجرایی کنترل سوابق، مدارک و مستندات سیستم مدیریت کیفیت	۱
SY-PR-02	روش اجرایی کنترل و نگارش مستندات سیستم مدیریت یکپارچه	۲

ECCIM.COM

