شرکت پالایش نفت امام خمینی (ره) شازند (سهامی عام)

روش اجرایی

مدیریت پسوردها و کنترل دسترسیهای حساس

فهـــــرست

1– هدف:

هدف از تهیه‌ی این رویه مستندسازی چگونگی مدیریت پسوردها و کنترل دسترسی به تجهیزات و سیستمهای حساس واحد فاوا در شرکت پالایش نفت امام خمینی (ره) شازند میباشد. ساختار ایجاد و کنترل دسترسیها باید به گونه ای باشد که همواره اطمینان از عدم ایجاد مشکل در دسترسی به سیستمهای حساس فراهم شود و شرکت در چرخه کار و اطلاعات؛ هیچگاه دچار مشکل وابستگی به اشخاص (کاربران کلیدی و راهبران سیستمها) نشود. این رویه بر اساس مفاد سند راهبردی امنیت اطلاعات شرکت و مبانی کنترل دسترسی در سیستمهای حساس (مبتنی بر پسورد) و نیز مبانی مدیریت و سرپرستی تهیه شده است.

2– حدود:

این دستورالعمل محدود به مسئولیت روسای واحدهای فاوا و حراست و تمامی کارکنانی است که دسترسی به تجهیزات سخت افزاری و سیستمهای نرم افزاری حساس شرکت پالایش نفت امام خمینی (ره) شازند دارند و پس از تصویب؛ در واحدهای فاوا و حراست لازم الاجرا میباشد.

3– مسئولیتها:

- مدیرعامل شرکت پالایش نفت امام خمینی (ره) شازند مسئولیت تصویب و ابلاغ این دستورالعمل و نظارت کلی بر اجرای آنرا برعهده دارد.
- روسای اداره استقرار و توسعه سامانه های مدی‌ری‌تی و واحد حراست شرکت پالایش نفت امام خمینی (ره) شازند براجرای این دستورالعمل نظارت دارند.
- ری‌ی‌س واحد فناوری اطلاعات و ارتباطات شرکت؛ مسئول اجرای این دستورالعمل در حوزه مسئولیت خود میباشد.
- کمیته امنیت اطلاعات شرکت مسئول بازنگری این دستورالعمل میباشد و وظیفه اعمال کنترلها و انجام هماهنگی های لازم در کاربرد دستورالعمل های مرتبط و بازنگری آنها در سطح شرکت را برعهده دارد.

4– منابع:

- سند راهبردی سیستم مدیریت امنیت اطلاعات شرکت پالایش نفت امام خمینی (ره) شازند
- رویه های مشابه موجود در سایر شرکتهای پالایشی

5–تعاریف:

جدول : تعاریف

عبارت	تعریف
سیستم مدیریت امنیت اطلاعات (ISMS[1])	قسمتی از سیستم مدیریت کلان، بنا شده بر دیدگاه مخاطرات کسب و کار، به منظور ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری، نگهداری و بهبود امنیت اطلاعات.
تجهی‌زات	هر گونه سخت افزار اعم از سرورها – کامپی‌وتر و لوازم جانبی آنها؛ مدی‌اهای ذخی‌ره سازی اطلاعات؛ قطعات و ملزومات شبکه کامپی‌وتری؛ امکانات مخابراتی و ارتباطی مورد استفاده برای انتقال و ی‌ا اشتراک اطلاعات و سای‌ر ابزارها و ی‌ا ادواتی که در اتاق سرور ی‌ا اتاقهای رک مورد استفاده قرار می‌گیرد.
شبکه	در یک تعریف ساده شبکه به مجموعه ای از دستگاه‌ها (کامپیوترها. ابزارها از جمله pad و ... و deviceها از جمله router، Hub، switch و ...) اطلاق می‌شود که به نوعی با هم در ارتباط هستند.
امنیت اطلاعات	محافظت از درستی و تمامیت اطلاعات
سیستمهای حساس	هر گونه سخت افزار و یا نرم افزاری که برای تامین امنیت اطلاعات اغلب مبتنی بر پسورد میباشند و لازمه دسترسی کاربران بدانها؛ در ابتدا تعریف/ایجاد دسترسی توسط ادمین یا نصاب سیستم میباشد.
دسترسی غیر مجاز	هر گونه دسترسی به منابع یا اطلاعاتی که توسط password یا سایر تدابیر امنیتی حفاظت شده و یا در مالکیت فرد نیست
ادمین سیستم	UserID که سیستم را نصب و یا پیکربندی می نماید و بالاترین سطح دسترسی به سیستم یا تجهیز را دارا میباشد و امکان ایجاد - مدیریت و کنترل دسترسی سایر کاربران به سیستم را دارد.
راهبر سرویس/سامانه	شخصی که وظیفه راهبری، مدیریت وتخصیص دسترسی‌های کاربران را بر عهده دارد
دسترسی ویژه	این نوع دسترسی، فراتر از حد کاربر عادی است. مجوز این دسترسی تنها از سوی رییس واحد فاوا (و با نظارت کارشناس حفاظت فاوای واحد حراست) تخصیص داده می‌شود

6– ضمانت اجرایی:

روسای اداره سامانه ها و واحدهای فاوا و حراست و کارکنان مرتبط با راهبری و مدیریت سیستمهای حساس در شرکت پالایش نفت امام خمینی (ره) شازند، موظف به رعایت مفاد این مستند هستند و در صورت بروز هر گونه تخلف در اجرای این سند، مطابق با مفاد "رویه انضباطی برخورد با موارد نقض امنیت اطلاعات" با شخص متخلف برخورد خواهد شد.

7– بازنگری :

ای‌ن سند در صورت بروز تغی‌ی‌راتی که بر آن تأثی‌ر گذارد، به منظور تضمی‌ن تناسب با نی‌ازمندی‌های شرکت مورد تجدی‌د نظر قرار خواهد گرفت.

[1] Information Security Management System

8- مراحل اجرا:

۸-۱- متولی نصب و پیکربندی تجهیز/سیستم/نرم افزار؛ بلافاصله پس از اتمام کار نصب و پیکربندی (حداکثر ۵ روز پس از آغاز عملیات نصب) و قبل از ایجاد دسترسی برای سایر کاربران؛ پسورد UserID ادمین اصلی هر سیستم (به عنوان مثال admin یا system و ...) را در اختیار رییس واحد فاوا قرار می دهد. رییس واحد فاوا بدوا نسبت به تغییر فوری پسورد ادمین اصلی اقدام می نماید. سپس برای خود یک UserID با دسترسی کامل ایجاد می نماید. با توجه به توصیه اکید سند راهبردی سیستم مدیریت امنیت اطلاعات شرکت؛ هر کاربر بایستی با UserID مجزای خاص خود از سیستمها استفاده نماید. همچنین رییس واحد فاوا یک UserID برای جانشین خود با دسترسی کامل (جهت مانیتورینگ فعالیت راهبران و کاربران و کنترل لاگها و دسترسیها) ایجاد و تحویل می نماید. بدیهی است که ایجاد دسترسی برای نفرات جانشین به این منظور است که هیچ گاه کار شرکت معطل نماند.

۸-۲- رییس واحد فاوا یک نسخه از پسوردهای UserID های ادمین اصلی سیستمها را در پاکت مهر و موم شده در اختیار رییس واحد حراست قرار میدهد تا در صورت نیاز در مواقع اضطراری مورد استفاده قرار گیرد. در صورت نیاز به استفاده از پسوردهای موجود در پاکت مهر و موم شده؛ بایستی مراتب باز شدن پاکت با حضور رییس حراست و مسئول حفاظت فاوای حراست و کارشناس استفاده کننده از سیستم؛ صورتجلسه شود. ضمنا هرگاه پسورد UserID اصلی ادمین سیستمها عوض شود؛ رییس واحد فاوا موظف است؛ پاکت مهر و موم شده قبلی را از حراست تحویل گرفته و پاکت جدید حاوی پسوردهای جدید را در اختیار رییس واحد حراست/کارشناس حفاظت فاوای حراست قرار دهد.

۸-۳- رییس واحد فاوا یک UserID با سطح دسترسی کامل/ هم ارز ادمین/بالاترین سطح دسترسی؛ برای راهبر سیستم ایجاد و پسورد آن را تحویل متولی راهبری سیستم می نماید. همچنین رییس واحد فاوا یک UserID برای فرد جانشین متولی سیستم (با دسترسی کامل) ایجاد و تحویل می نماید. در صورت حضور متولی اصلی؛ نفر جانشین لزومی ندارد وارد سیستم شود مگر برای کنترل لاگها و یا اجرای دستورات رییس واحد فاوا.

۸-۴- اگر سیستمی امکان اجرای سیاست سلسله مراتب دسترسی فوق را ندارد؛ توسط رییس واحد فاوا در مورد آن به صورت ویژه تصمیم گیری و موضوع با جانشین خود - متولی راهبری سیستم و فرد جانشین او صورتجلسه می شود.

۸-۵- ایجاد هرگونه دسترسی برای کارکنان به اطلاعات و سامانه‌های اطلاعاتی شرکت پالایش نفت امام خمینی نیازمند درخواست رییس واحد متقاضی است. هر کاربر باید به اندازه «نیازش نسبت به دانستن» و در خصوص تجهیزات در اختیار نیز باید به اندازه «نیازش نسبت به استفاده» به تجهیزات و سیستمها دسترسی داشته باشد. جهت ایجاد دسترسی برای کاربران معمولی سیستمها؛ درخواست ایجاد دسترسی توسط رییس واحد متقاضی به رییس واحد فاوا ارسال میشود. پس از ایجاد دسترسی؛ پسورد اولیه کاربر توسط رییس واحد فاوا به رییس واحد متقاضی ارسال و توسط ایشان به کاربر تحویل میشود. کاربر موظف است بلافاصله پس از تحویل گرفتن UserID خود نسبت به تغییر پسورد اولیه اقدام نماید. بر مبنای الزامات سند راهبردی امنیت اطلاعات؛ هیچ یک از همکارانی که پسورد سیستمها (مخصوصا سیستمهای حساس) را در اختیار دارند نباید پسورد خود را در اختیار دیگران قرار دهند.

۸-۶- جهت ایجاد اطمینان از عدم وجود کاربران و دسترسیهای اضافی؛ بایستی توسط راهبر هر سیستم/ جانشین او و یا رییس واحد فاوا/جانشین او؛ مرتبا و در فواصل زمانی کوتاه؛ ترجیحا هفتگی؛ لیست کاربران سیستمها و نحوه دسترسی آنها کنترل شود و در صورت وجود دسترسیهای خارج از چارچوب تعیین شده فوق؛ دسترسیهای اضافی قطع و موضوع گزارش شود.

۸-۷- اداره منابع انسانی موظف است هرگونه تغییرات در وضعیت پرسنل اعم از قطع همکاری – انتقال – تسویه – تغییر شغل و ... را بلافاصله به واحد فاوا منعکس نماید تا تغییرات لازم در دسترسی های پرسنل ایجاد شود. برای این منظور مطابق رویه/روش اجرایی مربوطه اقدام خواهد شد. در مورد کارکنانی که برای مدت بیش از یک ماه در محل کار حضور نخواهند داشت (مأموریت، مرخصی و ...)، واحد منابع انسانی باید مراتب را به واحد فناوری اطلاعات و ارتباطات اعلام نماید. پس از ارائه این ابلاغ، واحد فناوری اطلاعات و ارتباطات باید نام کاربری فرد را در سرویس‌ها و سامانه‌های اطلاعاتی غیرفعال نماید. همچنین پس از بازگشت فرد، علاوه برفعال سازی مجدد نام کاربری، نسبت به تغییرکلمه عبور نیز اقدام گردد. لازم به ذکراست باید برای افراد جدید جایگزین شده دسترسی جدید تعریف شود و از اعطای دسترسی فرد قبلی به کاربر جدید خودداری گردد.

۸-۸- در خصوص سیستمهایی که قبل از تصویب و ابلاغ این روش اجرایی نصب و پیکربندی و عملیاتی شده اند؛ لازمست حداکثر ظرف یک هفته پس از ابلاغ این روش اجرایی؛ اقدامات فوق به طور کامل انجام شود.

۸-۹- امنیت اطلاعات ایجاب می نماید که همواره راهبران و کاربران به صورت متناوب؛ در یک بازه زمانی معقول پسوردها را تغییر دهند. مسئولیت حفظ و نگهداری از اکانت و جلوگیری از سوء استفاده از دسترسیهای هر کاربر بعهده خود اوست. کاربران در حد امکان در مقابل چشم دیگران از ورود پسورد خودداری نمایند. همواره بلافاصله پس از اینکه حدس زدند یا احتمال دادند شخص دیگری پسورد را دیده؛ یا با ابزار دیگری پیدا کرده؛ بایستی نسبت به تغییر پسورد اقدام نمایند.

۸-۱۰- فرآیند اعطاء، تغییر یا حذف دسترسی به اطلاعات و سرویس‌های اطلاعاتی توسط کارشناس/مدیر واحد آغاز می‌گردد. ایشان باید درخواست خود را طی فرآیند داخلی سازمان (سامانه اتوماسیون اداری یا میز خدمات فاوا) به واحد فناوری اطلاعات و ارتباطات ارجاع نماید. رییس واحد فاوا ضمن بررسی؛ درخواست را جهت اقدام به کارشناس مربوطه ارجاع می‌نماید.

۸-۱۱- در صورت ضرورت کاری در شرایط خاص؛ اعطای دسترسی ویژه (از قبیل دسترسی از راه دور و ...) با صلاحدید رییس واحد فاوا و هماهنگی و نظارت کارشناس حفاظت فاوای حراست؛ انجام خواهد شد. دسترسی از راه دور به اطلاعات سرویس‌های اطلاعاتی شبکه اینترانت مجاز نیست و این دسترسی صرفاً در مواقع اضطراری اعطاء می‌گردد.

۸-۱۲- الزامات کنترل دسترسی

به طور جامع، در حد امکان موارد ذیل جهت رعایت الزامات نحوه کنترل دسترسی باید در نظر گرفته شود:

کاربر تنها دسترسی به تجهیزات و اطلاعاتی دارد که برای انجام وظایف خود (کارها/نقش‌های مختلف) نیازمند است؛

حقوق دسترسی مبتنی بر نقش سازمانی صورت پذیرد؛

به منظور کنترل بهتر شبکه؛ با استفاده از VLAN جداسازی صورت پذیرد؛

پس از نصب و راه اندازی تجهیزات سخت افزاری و شبکه مانند سوئیچ و نیز نرم افزارها، باید اطلاعات ورود اولیه (شامل نام کاربری و کلمه عبور پیش‌فرض) سیستم تغییر یابد؛

از شناسه منحصر به فرد برای کاربران جهت دسترسی به سرویس‌ها و منابع اطلاعاتی استفاده گردد (اختصاص شناسه مشترک بین چند کاربر تنها در صورتی که ضرورت کسب و کار شرکت ایجاب نماید و پس از اخذ تأییدیه و مستندسازی امکان پذیر است)؛

نام‌های کاربری تکراری شناسایی، لغو و یا مسدود گردد؛

شرایط و زمان اتمام حقوق دسترسی با امتیازات ویژه اعطاء شده تعیین گردد؛

اطلاعات احراز هویت محرمانه (نام کاربری و کلمه عبور) باید به شیوه ای امن در اختیار کاربران قرار گیرد. این اطلاعات باید منحصر به فرد و غیر قابل حدس زدن باشند؛

ایجاد رویه مناسب جهت ورود به سیستم یا برنامه کاربردی نظیر:

عدم نمایش پیغام‌های راهنمایی در طول فرآیند ورود به منظور جلوگیری از ورود کاربر غیرمجاز به سیستم؛

محافظت از سیستم در برابر تلاش‌های ورود غیرمجاز نظیر Lock شدن یا استفاده از Captcha؛

عدم نمایش کلمه عبور به هنگام وارد کردن آن در سیستم؛

استفاده از امکانات پایش و نظارت و ثبت وقایع جهت مشخص شدن ورود ناموفق؛

عدم قرار گرفتن هرگونه اطلاعات در صفحه احراز هویت تا قبل از ورود کاربران برای تجهیزات و سرویس‌ها؛

استفاده از اخطار و پیغام «فقط کاربران مجاز اجازه دسترسی دارند» در صفحه login تمامی سرویس‌ها و تجهیزات شرکت؛

۸-۱۳- کنترل دسترسی به سورس کد برنامه‌ها: جهت حفاظت از سورس کد برنامه ها باید مرکز ذخیره سازی کدها (مجموعه سورس برنامه ها) را با رعایت کلیه اقدامات و الزامات لازم؛ کنترل نمود.

۹– تاریخ تصویب واجرای این دستورالعمل:

این دستورالعمل با همکاری واحدهای فاوا و حراست در ۹ بند تهی‌ه و تدوی‌ن گردی‌ده و پس از تصوی‌ب و امضای مدی‌ر عامل شرکت پالایش نفت امام خمینی (ره) شازند در سطح واحدهای مرتبط لازم الاجرا می باشد.

نام و نام خانوادگی	سمت	تاری‌خ	امضا
مجید رجبی	مدیرعامل		
علی اکبر میرزایی مهر	رییس استقرار و توسعه سامانه های مدیریتی		
محمدرضا دهنمکی	رئیس حراست		
عباس خسروبیگی	رئیس فناوری و اطلاعات و ارتباطات		