طرح دیسپچینگ شرکت ملی پخش فرآورده‌های نفتی ایران

– سیاست امنیت اطلاعات شرکت‌های توزیع فرآورده

NIOPDC Dispatching Branding Security Policy

تهیه کننده/تهیه کنندگان	طرح سامانه دیسپچینگ شرکت ملی پخش فرآورده‌های نفتی ایران
تاریخ	۹۷/۷/۱۷
نسخه	۱,۰
مدت اعتبار	تا نسخه بعدی
نوع مستند	[infosec]
محل نگهداری	طرح دیسپچینگ
سطح محرمانگی	عمومی
امضاء تأیید کننده	

شناسنامه سند

نام سند	طرح دیسپچینگ شرکت ملی پخش فرآورده‌های نفتی ایران – سیاست امنیت اطلاعات شرکت‌های توزیع فرآورده NIOPDC Dispatching Branding Security Policy
نسخه	۱,۰
تاریخ آخرین انتشار	۹۷/۷/۱۷
نام تهیه کننده/تهیه کنندگان	طرح سامانه دیسپچینگ
سطح محرمانگی	عمومی
مستندات مرتبط	-

سابقه بروز رسانی

تاریخ بروزرسانی	نسخه
۹۷/۷/۱۷	۱,۰

فهرست

۱ هدف

هدف این سند، نیل به موارد زیر می‌باشد:

- کاهش ریسک‌های امنیت اطلاعات طرح دیسپچینگ شرکت ملی پخش فرآورده‌های نفتی ایران بالاخص در جایگاه و شرکت های توزیع فرآورده.
- اطلاعات جمع‌آوری شده به طور صحیح، حفاظت شده و در زمان مناسب در اختیار کسب و کار طرح دیسپچینگ قرار گیرند.
- حفاظت از دارایی‌های طرح دیسپچینگ در برابر تهدیدات امنیتی که تمامیت، محرمانگی، دسترس پذیری و اعتبار طرح را به خطر می‌اندازند.
- اطمینان از اینکه تمام افرادی که در چرخه استحصال اطلاعات مشارکت دارند، از قوانین و اصول امنیت اطلاعات مطلع بوده و به آنها عمل می‌کنند.
- بهبود مداوم امنیت اطلاعات براساس فیدبک افرادی که در چرخه استحصال اطلاعات مشارکت دارند، رخدادها و نتایج ممیزی‌ها
- اطمینان از رعایت سیاست‌های امنیت اطلاعات طرح دیسپچینگ و قوانین و احکام بالادستی شرکتی، دولتی و ملی.

۲ تعاریف

- **دارایی‌های طرح دیسپچینگ:** کامپیوتر دیسپچینگ مشتمل بر نرم‌افزارها، برد RTU، UPS، مانیتور، سیم کارت APN و اطلاعاتی که توسط این دارایی‌ها و کامپیوتر تجمیع اطلاعات در اتاق کنترل شرکت های توزیع فرآورده جمع‌آوری، پردازش و نگهداری می‌شوند.
- **ناظر طرح دیسپچینگ:** کسی یا کسانی که از سوی طرح دیسپچینگ شرکت ملی پخش به عنوان ناظر به شرکت‌های توزیع فرآورده معرفی می‌شوند.
- **افراد مجاز:**
  - در جایگاه: جایگاه دار و اپراتور جایگاه

- در اتاق کنترل شرکت های توزیع فرآورده: سه نفر از کارکنان شرکت های توزیع فرآورده که به عنوان نماینده شرکت های توزیع فرآورده برای اجرای دیسپچینگ (فنی و مدیریتی) به طرح دیسپچینگ معرفی شده‌اند.

۳ محدوده

محدوده این سند مشتمل است بر:

- جایگاه
- افراد مجاز
- شرکت های توزیع فرآورده
- اتاق کنترل شرکت های توزیع فرآورده
- هر اطلاعاتی که از طریق سه آیتم بالا جمع‌آوری، پردازش و ذخیره می‌شوند.

۴ سیاست امنیت اطلاعات جایگاه و اتاق کنترل شرکت های توزیع فرآورده طرح دیسپچینگ

۴,۱ کنترل فیزیکی و محیطی

- دارایی دیسپچینگ باید در اتاقی با مشخصات زیر قرار بگیرند:
  - ✓ قفل دار باشد.
  - ✓ به جز افراد مجاز، ورود افراد متفرقه ممنوع است.
  - ✓ تاریخ و ساعت ورود و خروج افراد در دفتری با عنوان "دفتر ورود و خروج" ثبت و تا یکسال نگهداری شود.
  - ✓ توصیه می‌شود که دوربین مدار بسته (با قابلیت ضبط تصویر و نگهداری آن تا حداقل ۳۰ روز) با دید کامل بر روی دارایی دیسپچینگ نصب شود.
  - ✓ تنها راه ورود و خروج، درب ورودی باشد.

- ✓ در و دیوارها پوشیده بوده و شفاف نباشند، همچنین، دید مستقیم از بیرون وجود نداشته باشد.
- ✓ الزامات HSE بخصوص درباره آتش سوزی، سیل و زمین لرزه رعایت شده باشند.
- ✓ شرایط استاندارد از لحاظ گرد و خاک، دما و رطوبت رعایت شده باشد.

- پس از نصب تجهیزات دیسپچینگ در محلی که طرح دیسپچینگ شرکت ملی پخش تأیید کرده است، هر گونه جابجایی و دستکاری تجهیزات ممنوع است.
- لیست دارایی‌های دیسپچینگ با ذکر شماره اموال/ شناسه باید یکبار ابراز و در اختیار طرح دیسپچینگ قرار گیرد.
- باید دارایی‌های دیسپچینگ، متمایز و مجزا از بقیه تجهیزات قرار داده شوند.
- کابل کشی باید مطابق با استاندارد بوده، داکت کشی، جداسازی داکت شبکه از برق با حفظ فاصله استاندارد صورت گرفته و تمام کابل‌ها برچسب گذاری و دسته‌بندی شده باشند.
- نباید دارایی دیسپچینگ و کابل کشی آنها در معرض تردد و آسیب باشند.
- زاویه قرارگیری صفحه نمایش به گونه‌ای باشد که افراد غیرمجاز نتوانند صفحه نمایش را ببینند.
- دور نگهداشتن غذا و نوشیدنی و امثال آنها از ایستگاه‌های کاری جهت پیشگیری از خسارات فیزیکی تصادفی.
- کشیدن سیگار در فضایی که دارایی‌های دیسپچینگ قرار دارد ممنوع است.
- کاغذ و یا هر نوع مدیای فیزیکی حاوی اطلاعات مربوط به طرح دیسپچینگ شرکت ملی پخش، در زمانی که استفاده نمی‌شوند باید در کمدی قفل دار گذاشته شوند.
- هرنوع تصویربرداری، ضبط صدا و یا هر نوع ضبط دیگری (حتی اسکرین شات) ممنوع است مگر اینکه از طرح دیسپچینگ شرکت ملی پخش مجوز اخذ شود.

۴,۲ کنترل نیروی انسانی

- تمام افراد مجاز جایگاه‌ها و شرکت های توزیع فرآورده باید سند عدم افشاء اطلاعات (NDA) امضاء نمایند، مبنی بر اینکه تعهد کنند که طبق سیاست‌ها و قوانین امنیت اطلاعات از اطلاعات استفاده

کرده و آنها را افشاء نکرده و یا به وسیله آنها خسارتی به شرکت ملی پخش و مجموعه صنعت نفت وارد نکنند (فرآیند مربوط به اخذ سند NDA متعاقبا اعلام خواهد گردید).

- کاربران بایستی به حساسیت نرم‌افزارهای و اطلاعاتی که با آن سر و کار دارند واقف بوده و احتمال دسترسی غیرمجاز را تا حد ممکن کاهش دهند.
- چنانچه کاربران موردی را می‌دانند یا مشاهده کرده‌اند که می‌تواند امنیت نرم‌افزارها را به خطر اندازد و یا اینکه احساس می‌کنند که از رمز عبور و سیستم سوءاستفاده می‌شود، باید به طرح دیسپچینگ شرکت ملی پخش اطلاع دهند.
- اگر نیاز به ورود شخصی غیرمجاز به اتاقی که دارایی های دیسپچینگ در آن قرار دارد باشد (به عنوان مثال برای تعمیرات)، حتما باید یکی از افراد مجاز تمام مدت وی را همراهی کرده، نظارت داشته و ورود و خروج فرد غیر مجاز نیز در "دفتر ورود و خروج" ثبت شود.
- هر سه ماه یکبار و نیز در زمان استخدام یا ترک کار افراد مجاز، باید لیست افراد مجاز بازبینی و بروز شود.
- به افراد مجاز، آموزش‌های لازم برای اجرای سیاست حاضر داده شود.

۴,۳ کنترل شبکه و ارتباطات

- نباید بر روی کامپیوتر LGTG، کامپیوتر دیسپچینگ و کامپیوتر یا سرور برند، کارت شبکه نصب باشد. در صورت وجود کارت شبکه Onboard بر روی مادربورد نیز، باید غیر فعال شود.
- اتصال به اینترنت و هر شبکه دیگری ممنوع است. همچنین، Network Interfaceهای Wifi، Bluetooth، Cellular، Infrared نیز باید غیرفعال شوند. شایان ذکر است که استفاده از شبکه بیسیم تحت هر شرایطی ممنوع است.

مبادی انتقال داده بجز از طریق بستر APN (از مبدأ جایگاه به مقصد شرکت ملی پخش/اتاق کنترل برند) باید غیرفعال بوده و هر نوع اتصال پورت USB خارج شده از برد RTU به هر وسیله‌ای بجز کامپیوتر دیسپچینگ ممنوع است.

۴,۴ کنترل سخت‌افزار

- پورتهای USB بسته باشند.
- امکان اتصال هیچ دستگاهی به سیستم وجود نداشته باشد. لازم است محدودیت‌ها (مثلا توسط آنتی ویروس) بر روی پورتهای USB صورت پذیرد به نحوی که کاربر در هیچ شرایطی نتواند از آنها استفاده غیرمجاز داشته باشد.
- پشت کیس ها می بایست پلمپ باشد به نحوی که اگر کاربر قصد انتقال اطلاعات توسط روش هارد به هارد را داشته باشد این موضوع قابل تشخیص باشد.
- دستگاه فاقد Floppy Drive باشد.
- اتصال هر نوع دستگاه جانبی (مانند هارد اکسترنال، فلش مموری، دانگل و غیره) به دارایی‌های دیسپچینگ ممنوع است.
- وجود رمز عبور برای ورود به Bios سیستم
- باید Bios بگونه‌ای پیکربندی شود که فقط از Local Hard Disk، Boot شود.
- کابل برق روی برد RTU باید پلمپ باشد.
- اتصالات سریال در سمت برد RTU و LGTG باید پلمپ باشند.
- همواره باید اتصال سریال کامپیوتر LG/TG با برد RTU برقرار بوده و مسئولیت آنها به عهده جایگاه می‌باشد.
- همواره باید برق برد RTU متصل بوده و در زمان قطعی برق جایگاه، UPS در مدار باشد. مسئولیت این امر به عهده جایگاه است.
- بر روی کامپیوتر LG/TG تنها پورت سریال فعال بوده و بقیه پورتها باید غیرفعال باشند.

۴,۵ کنترل نرم‌افزار و سیستم عامل

- سیستم عامل
  - ✓ دسترسی افراد مجاز باید در حداقل سطح ممکن یعنی سطح Need-to-Know باشد.

- ✓ تمام سرویس‌های سیستم عامل که مشارکتی در عملکرد نرم‌افزار جایگاه سفید و نرم‌افزار تجمیع اطلاعات شرکت های توزیع فرآورده نداشته و برای کار کردن (بالا ماندن) سیستم عامل ضروری نیستند، باید غیرفعال شوند(با تأکید بر روی RDP و Telnet).
- ✓ نصب Telnet ممنوع است.
- ✓ دسترسی به سرویس‌ها و رجیستری سیستم عامل تنها برای ادمین مجاز است و برای دیگر افراد باید غیرفعال باشد.
- ✓ تمام پورت‌های USB غیرفعال شوند. باید نرم‌افزار سفید بجز اطلاعاتی که از پورت USB نوع B که از برد RTU خارج شده، هیچ اطلاعات دیگری را نتواند بخواند.
- ✓ عدم استفاده از سیستم عامل و نرم افزارهای منقضی شده مانند Windows XP,Windows 2003
- ✓ دسترسی به Safe Mode و هر حالت دیگری به جز حالت نرمال بالا آمدن ویندوز، باید غیرفعال باشد.
- ✓ در صورتی که فعال سازی فایروال ویندوز اخلالی در نرم‌افزارها ایجاد نمی‌کند، فایروال ویندوز فعال باشد.
- ✓ باید Screen Saver با رمز عبور و زمان حداکثر ۱۰ دقیقه فعال باشد.
- ✓ هر فرد مجاز پس از اتمام کار، باید آن Session را ببندد.
- ✓ تاریخ و ساعت سیستم باید بروز باشد.
- ✓ توصیه می‌شود، سیستم عاملی که در اتاق کنترل شرکت های توزیع فرآورده، هاست تجمیع اطلاعات است، Windows Server 2012 R2 باشد.
- ✓ نباید بر روی کامپیوتر دیسپچینگ و کامپیوتر یا سرور شرکت های توزیع فرآورده، بیش از یک سیستم عامل نصب باشد و از نرم افزارهایی مانند VM Ware یا Virtual Box بر روی سیستم استفاده نشده باشد.
- ✓ بر روی کامپیوتر LGTG و کامپیوتر دیسپچینگ تنها یک درایو C:\ وجود داشته باشد. تنها ادمین بر روی این درایو دسترسی کامل داشته و دیگر افراد مجاز فقط دسترسی Read داشته باشند.
- ✓ حصول اطمینان از اینکه ایستگاه‌های کاری تنها برای اهداف کاری مجاز استفاده شده و برای مقاصد شخصی استفاده نمی‌شوند.

- ✓ در صورت وجود داده‌های حساس بر روی ایستگاه کاری، لازم است از این اطلاعات نسخه پشتیبان تهیه شود و مسئولیت پی گیری و حصول اطمینان از انجام آن با کاربر است.
- ✓ تنها نرم‌افزار جایگاه سفید بر روی کامپیوتر دیسپچینگ جایگاه نصب بوده و قابل استفاده باشد. نصب هر نرم‌افزار دیگری ممنوع است و باید این امر غیرفعال باشد (آنتی ویروس مشمول این بند نیست).
- ✓ تنها نرم‌افزارهای مورد نیاز (ترجیحا بدون همپوشانی عملکرد) جهت تجمیع داده دیسپچینگ بر روی کامپیوتر یا سرور اتاق کنترل شرکت های توزیع فرآورده نصب بوده و قابل استفاده باشد. نصب هر نرم‌افزار دیگری ممنوع است و باید این امر غیرفعال باشد (آنتی ویروس مشمول این بند نیست).
- ✓ زمانی که از نرم‌افزار جایگاه سفید یا نرم‌افزار تجمیع داده دیسپچینگ استفاده نمی‌شود، باید سیستم عامل قفل شود.
- ✓ کد نرم‌افزار جایگاه سفید و یا نرم‌افزار تجمیع اطلاعات شرکت های توزیع فرآورده نباید قابل مشاهده و در دسترس باشد.
- ✓ اطلاعات استحصال شده توسط نرم‌افزار جایگاه سفید تنها باید قابل نمایش برای افراد مجاز جایگاه و منطقه بوده و هر نوع کپی، تغییر و نمایش دیگری از آن ممنوع است.
- ✓ اطلاعات تجمیع شده توسط نرم‌افزار تجمیع اطلاعات شرکت های توزیع فرآورده نباید تغییر کرده یا افشاء شوند.

➢ آنتی ویروس و وصله‌های امنیتی

- ✓ آنتی ویروس نصب بوده و بروز باشد.
- ✓ بروز رسانی آنتی ویروس به صورت آفلاین صورت گیرد.
- ✓ آنتی ویروس باید حداقل در ۲ روز گذشته به روزرسانی شده باشد.
- ✓ انجام عملیات Full Scan توسط آنتی ویرس به صورت هفتگی یا حداقل دو هفته یک بار.
- ✓ وصله‌های امنیتی ماهی یکبار به صورت آفلاین توسط ادمین نصب شوند.
- ✓ تنها ادمین می‌تواند برای نصب وصله‌های امنیتی، بروز رسانی آنتی ویروس و بروز رسانی نرم‌افزار جایگاه سفید یا نرم‌افزار تجمیع اطلاعات شرکت های توزیع فرآورده، به طور موقت

و تا اتمام بروزرسانی، یک پورت USB را باز کند؛ پس از آن باید مجددا پورت را غیرفعال کرده و اجازه انتقال هیچ داده دیگری بجز موارد مذکور را نیز ندارد.

- ✓ فلش مموری‌ای که برای بروز رسانی آنتی ویروس، وصله‌های امنیتی، نرم‌افزار جایگاه سفید یا نرم‌افزار تجمیع اطلاعات شرکت های توزیع فرآورده بکار می‌رود باید هر بار ابتدا فرمت شده، سپس اطلاعات مذکور بر روی آن انتقال داده شود. توجه شود که باید سیستمی که اطلاعات از روی آن بر روی فلش مموری کپی می‌شود، با آنتی ویروس بروز، اسکن شده باشد.

- ➢ شناسه کاربری و رمز عبور

- ✓ شناسه کاربری و رمز عبور هر یک از افراد مجار باید یکتا بوده و با حداقل ممکن دسترسی یعنی سطح دسترسی Need-to-Know باشد.
- ✓ شناسه کاربری و رمز عبور افراد مجاز نباید به صورت اشتراکی استفاده شود.
- ✓ کامپیوتر دیسپچینگ و کامپیوتر یا سرور اتاق کنترل شرکت های توزیع فرآورده، نباید بیش از یک کاربر ادمین داشته باشند.
- ✓ هر رمز عبوری باید پیچیدگی زیر را داشته باشد:
  - حداقل طول مجاز ۸ و حداکثر طول مجاز ۳۰ کاراکتر باشد.
  - شامل عدد، حروف کوچک و بزرگ و علامت‌های خاص باشد.
  - مشابه رمز عبور قبلی یا نام کاربری نباشد.
- ✓ پس از اولین ورود به سیستم باید رمز پیش فرض، الزاما تغییر کند.
- ✓ امکان ذخیره رمز عبور غیر فعال شود.
- ✓ پس از سه بار تلاش ناموفق متوالی نام کاربری، آن نام کاربری برای ۳۰ دقیقه غیرفعال شود.
- ✓ شناسه کاربری افراد مجازی که ترک کار می‌کنند باید پاک شود.
- ✓ تنها شناسه کاربری افراد مجاز و ادمین بر روی سیستم عامل فعال بوده و وجود داشته باشد.

- ➢ لاگ

- ✓ تمام لاگ‌های سیستمی و امنیتی از جمله لاگ‌های ادمین فعال بوده و تا حداقل سه ماه نگهداری شوند. لاگ‌ها تا پیش از سه ماه نباید پاک شده یا تغییر داده شوند.
- ✓ لاگ تمام ورود و خروج‌های سیستمی ثبت و نگهداری شود.

۴,۶ کنترل تغییرات

- ➢ تغییرات، تعمیرات و هر نوع خطا یا اتفاق یا حادثه‌ای که رخ می‌دهد به همراه اقدامات صورت گرفته، باید در دفتری با عنوان "دفتر وقایع" ثبت و تا دو سال نگهداری شوند.
- ➢ به ازاء هر تغییر و یا تعمیر دارایی‌های دیسپچینگ باید ابتدا از طرح دیسپچینگ شرکت ملی پخش مجوز گرفته شده و پس از انجام آن، صورتجلسه‌ای بین طرفین و با حضور شرکت پخش تنظیم شده و امضاء شود. همچنین در "دفتر وقایع" نیز باید ثبت شود.
- ➢ خروج و ارسال هر دارایی دیسپچینگ جهت تعمیرات با شرایط زیر باید صورت گیرد:
  - ✓ پیش از ارسال، از طرح دیسپچینگ شرکت ملی پخش مجوز گرفته شده باشد.
  - ✓ پیش از ارسال، از اطلاعات حیاتی آن پشتیبان گرفته شده و آن اطلاعات پاک شده باشند.
  - ✓ پس از بازگشت از تعمیر، باید تست امنیتی جهت حصول اطمینان از صحت عملکرد و دستکاری نشدن آن صورت گرفته و به همراه شرح مختصری از اقدامات انجام شده، رکوردی در "دفتر وقایع" ثبت شود.
  - ✓ زمان و تاریخ ورود و خروج آن در "دفتر وقایع" ثبت شود.

۵ مخاطبین (Users)

تمام محدوده، مخاطب این سند هستند.

۶ مالک سیاست (Policy Owner)

مجری طرح دیسپچینگ، صاحب سیاست‌ها هستند.

۷ تایید سیاست (Policy Approval)

مجری طرح دیسپچینگ مسئول تایید سیاست است. وی باید پس از تایید، سیاست را به محدوده ابلاغ کند. بدیهی است که پس از ابلاغ سیاست، تمامی محدوده مشمول شده و لازم الاجرا می‌باشند. در صورت مشاهده هر گونه عدم همکاری و یا تخطی در اجرای سیاست و یا نقض امنیت اطلاعات، مراتب باید به مجری طرح دیسپچینگ گزارش شده تا بررسی و مطابق با قوانین با افراد خاطی برخورد شود.

۸ بازنگری سیاست و اعتبار سند (Policy Review)

این سیاست تا نسخه بعدی که از سوی طرح دیسپچینگ شرکت ملی پخش ابلاغ گردد، اعتبار داشته و لازم‌الاجرا می‌باشد.

۹ الزامات سیاست (Policy Obligations)

تمام دستورالعمل‌ها، روال‌ها و اقدامات امنیتی صورت گرفته باید مطابق با سیاست حاضر باشند.

۱۰ تطابق با سیاست

۱۰,۱ معیار تطابق

ناظر طرح دیسپچینگ شرکت ملی پخش تطابق وضع جاری جایگاه‌ها و اتاق کنترل شرکت های توزیع فرآورده را با سند حاضر با استفاده از روش‌هایی مانند بازدیدهای منظم و نامنظم، گزارش، مانیتورینگ و بازتاب عمومی به سند حاضر، ارزیابی می‌کند.

۱۰,۲ استثناءها

هر نوع استثناء در اعمال سند حاضر باید ابتدا توسط مجری طرح دیسپچینگ تصویب شود.

۱۰,۳ عدم انطباق

با کسی یا کسانی که از سند حاضر تخطی کنند مطابق با قوانین و مقررات حقوقی شرکت ملی پخش برخورد خواهد شد.

۱۱ منابع

- سند سیاست‌های امنیت اطلاعات طرح دیسپچینگ
- سند جمع‌بندی مستندات احکام امنیتی حراست، افتا و پدافند غیرعامل

۱۲ تأییدیه‌ها

سمت	نام و نام خانوادگی	تاریخ	امضاء

تعهدنامه دوجانبه محرمانگی

Non-Disclosure Agreement

تهیه کننده/تهیه کنندگان	طرح سامانه دیسپچینگ شرکت ملی پخش فرآورده‌های نفتی ایران
تاریخ	۹۷/۸/۹
نسخه	۱,۰
مدت اعتبار	نامحدود
نوع مستند	[infosec]
محل نگهداری	Kazemi-pc, soheili-pc, Hajighavami-pc
سطح محرمانگی	عمومی
امضاء تأیید کننده	

شناسنامه سند

نام سند	قرارداد دوجانبه محرمانگی Non-Disclosure Agreement
نسخه	۱,۰
تاریخ آخرین انتشار	۹۷/۸/۹
نام تهیه کننده/تهیه کنندگان	طرح سامانه دیسپچینگ
سطح محرمانگی	عمومی
مستندات مرتبط	-

سابقه بروز رسانی

تاریخ بروزرسانی	نسخه
۹۷/۸/۹	۱,۰

قرارداد دوجانبه محرمانگی
Non-Disclosure Agreement

نسخه ۱,۰
۹۷/۸/۹

این پیمان بین شرکت ملی پخش فرآورده‌های نفتی ایران به شماره ملی/ ثبت ..... به آدرس: ..... به شماره تلفن ..... که ازاین‌پس در این قرارداد صاحب اطلاعات نامیده می‌شود از یک طرف و شرکت / آقا/خانم ..... ثبت‌شده به شماره ..... در اداره ثبت شرکت‌ها و موسسات غیرتجاری و دارای شناسه ملی به شماره ..... و کد اقتصادی به شماره ..... به نمایندگی آقای ..... به شماره ملی ..... به سمت مدیرعامل و آقای ..... به شماره ملی ..... به سمت ..... به نشانی: .....؛ که طبق روزنامه‌های رسمی به شماره ..... مورخ ..... حق امضاء قرارداد را دارد از طرف دیگر و من‌بعد در این قرارداد به‌عنوان (گیرنده اطلاعات) خوانده می‌شود به شرح زیر منعقد می‌شود:

۱- **تعریف اطلاعات محرمانه:** بر این اساس " اطلاعات محرمانه " به معنی هرگونه اطلاعات فنی و غیر فنی مرتبط با طرح دیسپچینگ شرکت ملی پخش فرآورده‌های نفتی ایران است که بوسیله هر یک از طرفین به دیگری ارائه می شود.

۲- **شناسایی[۱] اطلاعات محرمانه:** اگر اطلاعات محرمانه در برگیرنده مدارک مشهود (شامل و نه محدود به نرم افزار, سخت افزار , نقشه ها, نمودارها[۲], جداول , دیسکها, نوارها, نمونه های اولیه [۳]و الگوها) باشد می توان آنها را محرمانه قلمداد نمود و حتی شرح مشابهی از آنها نیز اطلاعات محرمانه می باشد. اگر این اطلاعات محرمانه به صورت لسانی یا بصری افشاء شوند می توان آن را به عنوان افشاء اطلاعات در بازه زمانی محرمانگی شناخت.

۳- **موارد استثناء در اطلاعات محرمانه:** تعهدات هر یک از طرفین بر اساس این توافق نامه, در ارتباط با هربخشی از اطلاعات محرمانه طرف دیگر زمانی فسخ خواهد شد که طرف گیرنده اطلاعات به صورت مستند ثابت کند که: الف)زمانی که اطلاعات طرف دیگر قرارداد, به گیرنده اطلاعات آن انتقال داده شد آن اطلاعات

---

[۱] - Identification
[۲] - Graphs
[۳] - Prototypes

در معرض عموم بوده باشند. ب) اگر اطلاعات بواسطه طرف دیگر قرارداد در بازه زمانی محرمانگی در معرض عموم قرار بگیرد و گیرنده اطلاعات در این رابطه تقصیری نداشته باشد. ج) زمانی که اطلاعات در مالکیت گیرنده اطلاعات باشد و هیچ تعهدی در مورد محرمانه بودن نداده باشد و طرف دیگر قرارداد اطلاعات را بدون اخذ تعهد به ایشان منتقل کرده باشد د) زمانی که طرف دیگر قرارداد اطلاعات را به نحو مقرر به گیرنده اطلاعات آن منتقل کرده باشد ه) زمانی که اطلاعات بوسیله کارکنان و عوامل گیرنده اطلاعات آن به طور مستقل توسعه داده شود , بدون رجوع به اطلاعات رد و بدل شده فی مابین طرف قرارداد و گیرنده اطلاعات محرمانه و) زمانی که اطلاعات بوسیله طرف دیگر قرارداد به شخص سوم غیرمرتبط ارائه شده باشند بدون اینکه تعهدات محرمانگی فی مابین آنها ایجاد شده باشد. ز) زمانی که افشاء اطلاعات بدلیل صدور حکم دادگاه معتبر یا دیگر نهادها و سازمانهای دولتی بر اساس قانون موجود یا به منظور احصاء حقوق یکی از طرفین این قرارداد صورت گرفته باشد. ح) اگر در زمان افشاء اطلاعات، این اطلاعات به عنوان محرمانه مشخص نشده باشند و توسط طرف دیگر به صورت لسانی و بصری افشا شوند در زمان افشاء, این اطلاعات به عنوان اطلاعات محرمانه تلقی نخواهد شد.

۴- راهبری اطلاعات محرمانه:

هر طرف قرارداد توافق می نماید که در همه وقت و علی رغم پایان و انقضاء این قرارداد، کاملا" محرمانگی اطلاعات محرمانه طرف دیگر قرارداد را حفظ نماید و آن را برای طرف سومی مگر با توافق کتبی طرف دوم افشاء ننماید و اطلاعات محرمانه را برای هیچ هدف دیگری به غیر از موارد توافق شده کتبی با طرف دوم در این توافقنامه استفاده نخواهد نمود.

هر طرف فقط وقتی اجازه دسترسی به اطلاعات محرمانه را به طرف دیگر میدهد که استفاده کننده از کارکنانش بوده یا نماینده مجاز نیاز به دانستن آن داشته و کسی باشد که قرارداد محرمانگی را امضاء کرده یا اینکه ملزم به رعایت تعهدات محرمانگی حداقل محدود به محتوای ذکر شده در اینجا باشد.

۵- **دانش باقی مانده در ذهن:** گیرنده اطلاعات ممکن است زمانی که دانش و تجربه مربوط به خود یا شرکتش را افزایش می دهد این دانش حفظ شده به شکل نامحسوس در ذهن کارکنان، گردانندگان، پیمانکاران و مشاوران باقی بماند. بنابراین این اطلاعات به عنوان اطلاعات محرمانه افشاء شده تلقی می شوند. مادامی که گیرنده از بخش ۴ این توافقنامه تبعیت می نماید ممکن است وی نوعی از دانش، تجربه و یا مالکیت فکری

که می تواند به صورت عمومی مشابه به اطلاعات محرمانه باشد را توسعه، افشاء، بازاریابی، انتقال و یا استفاده نماید. دراین صورت دهنده اطلاعات هیچ گونه حقی در این نوع دانش، تجربه و مالکیت فکری ندارد. همچنین هیچ حقی مبنی بر اخذ غرامت مرتبط با استفاده از این نوع دانش، تجربه و مالکیت فکری نداشته و همینطور گیرنده هیچ حقی از مناسبات تجاری دهنده اطلاعات نخواهد داشت.

۶- مدت و تاریخ انقضاء قرارداد: این قرارداد از تاریخ تنفیذ تا مادامی که از سامانه دیسپچینگ استفاده می‌شود، ادامه خواهد یافت. تعهدات گیرنده اطلاعات بر اساس این قرارداد تا پایان مهلت قرارداد فی مابین باقی می مانند و حتی توسط وراث، جانشینان وافرادی که کار به آنها واگذار شده، الزام آور و غیر قابل فسخ می باشد. بمحض پایان و انقضاء مهلت قرارداد یا بمحض درخواست کتبی طرف دیگر قرارداد، طرف گیرنده باید فورا" تمامی مدارک، مستندات، مواد محسوس و نیز تمامی رونوشت های آنها که نشانه محرمانگی اطلاعات است را به طرف دهنده بازگرداند.

۷- تضمینها: هر طرف قرارداد به طرف دیگر اعلام و تضمین می نماید که الف) امتیاز حقوقی لازم برای وارد شدن و اجرای این قرارداد را دارا می باشد. ب) این قرارداد شامل تعهدات الزام آور حقوقی می باشد که مطابق با مدت آن قابل اجرا است. ج) روش انجام و اجرا بر اساس قرارداد شامل افشاءسازی اطلاعات محرمانه برای گیرنده آنها منتج به هیچ تعهد یا تخلف از تعهدی و یا نقض عهد نشده و یا تضییع حقوق در ارتباط با طرف سوم نخواهد شد.

۸- منع مهندسی معکوس: هر کدام از طرفین قرارداد توافق می نمایند که برنامه های نرم افزاری طرف دیگر دارای اطلاعات محرمانه ارزشمند است و هر طرف توافق می نماید که از تغییر، مهندسی معکوس، شکستن قفل نرم افزاری، خلق هر اثر دیگری مبتنی برآن و استفاده مجدد غیر مجاز از برنامه های نرم افزاری در اطلاعات محرمانه اجتناب نماید و بدون رضایت کتبی اولیه طرف دیگر قرارداد اقدام به انجام این امور ننماید.

۹- عدم اعطای حقوق: طرفین توافق کرده و می پذیرند که اطلاعات افشاء شده محرمانه متعاقب این توافقنامه هیچ گونه امتیاز یا حقوق مالکیتی برای طرف دیگر ایجاد نخواهد کرد و همچنین طرفین هیچ حقی از اختراع، ثبت اختراع، کپی رایت، علایم تجاری و دیگر حقوق مالکیت فکری که براساس این اطلاعات محرمانه بوجود آمده یا می آیند، ندارند. همچنین هیچ یک از طرفین حق ندارد هیچ محصول یا دیگر موارد استفاده

شده، ثبت شده و منتج از اطلاعات محرمانه طرف دیگر قرارداد را به هر منظوری ساخته، استفاده نموده یا بفروشد.

۱۰- جبران خسارات عادلانه: گیرنده اطلاعات اذعان می دارد که تخطی از این توافقنامه می تواند ضررهای جبران ناپذیری به دهنده اطلاعات وارد نماید که به دلیل آن دهنده اطلاعات محق به پیگیری قانونی جبران خسارات عادلانه و جبران ضررهای مالی است.

۱۱- متفرقه: هیچ طرفی بدون رضایت کتبی طرف دیگر نمی تواند این قرارداد را به طرف سوم یا نهاد دیگری انتقال یا واگذار نماید خواه در اجرای قانون باشد و یا به نحو دیگر. هر گونه تلاش بعمل آمده در موارد فوق فاقد اعتبار بوده و نافذ نمی باشد. هر گونه کنترل، اجرا، تفسیر و ترجمه این توافقنامه تابع قوانین جاری جمهوری اسلامی ایران است. طرفین توافق می نمایند که رضایت خود را از دادرسی در کشور جمهوری اسلامی ایران اعلام دارند. اگر بوسیله مرجع ذیصلاح بندهایی از این توافقنامه غیر قابل اجرا و بی اعتبار تشخیص داده شود، به طور کلی این عدم قابلیت اجرا و بی اعتباری، کل این توافقنامه را بی اعتبار و غیر قابل اجرا نخواهد کرد و در این حالت بندهای مذکور با نزدیکترین قانون قابل انطباق با اهداف این بندها تغییر کرده و تفسیر می شوند. هیچ طرفی حق واگذاری یا انتقال تعهدات مندرج در این توافقنامه را حتی با استنادات قانونی بدون رضایت کتبی طرف اول ندارد. این توافقنامه یک قرارداد کامل و انحصاری در مورد افشاء اطلاعات محرمانه

می باشد و جایگزین هر مکاتبه کتبی یا شفاهی قبلی فی مابین طرفین راجع به محرمانگی اطلاعات می باشد. این قرارداد ممکن است در چند نسخه امضاء شود و هر کدام از نسخه ها حکم واحد را دارد و پس از انعقاد قرارداد هر تکثیر معتبری از این توافقنامه حکم نسخه اصلی را دارد.

گواهی می شود, طرفینی که این قرارداد دوجانبه محرمانگی را ایجاد نموده اند از تاریخ تنفیذ آن را اجرایی نمایند.

بوسیله:.....بوسیله:.....

تاریخ:.....تاریخ:.....

آدرس:.....آدرس:.....

امضاء:.....امضاء:.....

بسمه تعالی

شرکت ملی پخش فرآورده‌های نفتی ایران
"حمایت از کالای ایرانی"

تاریخ ۱۳۹۷/۰۸/۱۵
شماره ۲۰ / ۱۳۲۱۹۵
پیوست

مدیران عامل محترم شرکت‌های زنجیره‌ای توزیع فرآورده

موضوع : اطلاعیه امنیت اطلاعات شماره ۱ – سیاست‌های امنیت اطلاعات شرکت‌های توزیع فرآورده

با سلام و احترام

با عنایت به نقش شرکت های زنجیره ای توزیع فرآورده در فرآیند استحصال اطلاعات جایگاه های عرضه سوخت کشور و همچنین اهمیت اطلاعات این حوزه از جنبه سایبری و امنیتی؛ از این پس سیاست‌ها، دستورالعمل‌ها و روال‌های امنیتی طی اطلاعیه‌های امنیت اطلاعات ابلاغ خواهند گردید و از زمان ابلاغ ، محتوای آن لازم الاجرا بوده و در بازه‌های زمانی از پیش تعیین شده، شرایط امنیتی شرکت‌ها مورد ممیزی قرار خواهند گرفت. لازم به ذکر است که این نامه به همراه ضمائم در سایت شرکت بارگذاری میگردد.

حامد کاظمی
از طرف مجری طرح دیسپچینگ

رونوشت : مدیر محترم مهندسی و طرح ها جهت استحضار لطفا.
: مدیر محترم بازرگانی جهت استحضار لطفاً
: مدیران محترم مناطق جهت استحضار لطفاً- شایان ذکر می باشد دستورالعمل های اجرایی این حوزه متعاقباً ابلاغ خواهد گردید-
: روسای محترم امور حقوقی و حراست جهت استحضار لطفاً
: رئیس پشتیبانی فنی جهت استحضار لطفا

تهران- خیابان ایرانشهر شمالی- نبش خیابان شاداب- شرکت ملی پخش فرآورده‌های نفتی ایران تلفن ۸۴۱۲۹-۰۲۱ نمابر: ۲-۸۸۸۱۳۱۱۱
WWW.NIOPDC.IR

مستندات و دستورالعمل های اجرایی شرکتهای زنجیره ای توزیع

1. **اصلاحیه دستورالعمل احداث جایگاه توسط شرکت‌های زنجیره ای توزیع ۲۱/۰۳/۹۶**
2. **فرآیند انعقاد قرارداد شرکت ملی پخش فرآورده های نفتی ایران با شرکتهای زنجیره ای توزیع**
3. **دستورالعمل الزامات جایگاه های تحت پوشش شرکت های صاحب نشان (مشتمل بر چک لیستهای الزامات جایگاه ، طرح کهاب و دیسپچینگ) ۹۶-۶-۲۶_**
4. *فرم ساماندهی پذیرش درخواست جایگاه داران جهت ورود به شرکت زنجیره ای توزیع (تکمیل و ارسال این فرم به همراه فرم گواهی نازل از تاریخ ۲۷/۰۱/۹۷ الزامی می باشد.*
5. *تاریخ اعتبار فرمهای گواهی نازل لینک دانلود*
6. **دستورالعمل الزامات جایگاه های تحت پوشش شرکت های صاحب نشان (مشتمل بر چک لیستهای الزامات جایگاه ، طرح کهاب و دیسپچینگ) ۹۶-۶-۲۶_**

7. **دستورالعمل فنی اجرایی طرح کهاب ۲۴/۱۱/۹۶**
8. **نمونه قرارداد شرکتهای زنجیره ای توزیع ویرایش ۲۱/۰۵/۹۷ لینک دانلود**
9. **دستورالعمل کنترل کیفیت فرآورده های نفتی شرکت های زنجیره ای توزیع سوخت**
10. **دستورالعمل آزمایش کمیت نازل های فروش مجاری عرضه تحت پوشش شرکتهای زنجیره ای توزیع**
11. **دستور العمل اجرایی طرح دیسپچینگ در جایگاه های عرضه سوخت ویرایش هشتم آبان ۹۸ (ینک دانلود)**
12. **اطلاعیه امنیت اطلاعات شماره ۱ طرح دیسپچینگ_(لینک دانلود)**

دستورالعمل ها و مستندات ساخت جایگاه های سوخت

13-محل های پیشنهادی جهت ساخت جایگاه سوخت در کشور

اصلاحیه دستورالعمل احداث جایگاه توسط شرکت‌های زنجیره ای توزیع ۲۱/۰۳/۹۶

14 .دستورالعمل ساخت جایگاه های سوخت کوچک و معمولی

15-Design, construction, modification, maintenance and decommissioning of filling stations ,

3rd edition