



## طرح دیسپچینگ شرکت ملی پخش فرآورده های نفتی ایران

– سیاست امنیت اطلاعات شرکت های توزیع فرآورده

### NIOPDC Dispatching Branding Security Policy

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



نسخه ۱,۰  
۹۷/۷/۱۷

طرح دیسپچینگ شرکت ملی  
پخش فرآورده های نفتی ایران -  
سیاست امنیت اطلاعات شرکت های  
توزیع فرآورده

## شناسنامه سند

نام سند	طرح دیسپچینگ شرکت ملی پخش فرآورده های نفتی ایران - سیاست امنیت اطلاعات شرکت های 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	-



طرح دیسپچینگ شرکت ملی  
پخش فرآورده های نفتی ایران -  
سیاست امنیت اطلاعات شرکت های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

## سابقه بروز رسانی

نسخه	تاریخ بروز رسانی
۱,۰	۹۷/۷/۱۷



طرح دیسپچینگ شرکت ملی  
پخش فرآورده های نفتی ایران -  
سیاست امنیت اطلاعات شرکت های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

## فهرست

۱ هدف	۶
۲ تعاریف	۶
۳ محدوده	۷
۴ سیاست امنیت اطلاعات جایگاه و اتاق کنترل شرکت های توزیع فرآورده طرح دیسپچینگ	۷
۴,۱ کنترل فیزیکی و محیطی	۷
۴,۲ کنترل نیروی انسانی	۸
۴,۳ کنترل شبکه و ارتباطات	۹
۴,۴ کنترل سختافزار	۹
۴,۵ کنترل نرمافزار و سیستم عامل	۱۰
۴,۶ کنترل تغییرات	۱۳
۵ مخاطبین (Users)	۱۴
۶ مالک سیاست (Policy Owner)	۱۴
۷ تایید سیاست (Policy Approval)	۱۴
۸ بازنگری سیاست و اعتبار سند (Policy Review)	۱۴
۹ الزامات سیاست (Policy Obligations)	۱۴
۱۰ تطابق با سیاست	۱۵
۱۰,۱ معیار تطابق	۱۵
۱۰,۲ استثناءها	۱۵

نسخه ۱,۰  
۹۷/۷/۱۷



طرح دیسپچینگ شرکت ملی  
پخش فرآورده های نفتی ایران -  
سیاست امنیت اطلاعات شرکت های  
توزیع فرآورده

۱۰,۳ عدم انطباق..... ۱۵

۱۱ منابع..... ۱۵

۱۲ تأییدیه ها..... ۱۵



## ۱ هدف

هدف این سند، نیل به موارد زیر می باشد:

- کاهش ریسک های امنیت اطلاعات طرح دیسپچینگ شرکت ملی پخش فرآورده های نفتی ایران بالاخص در جایگاه و شرکت های توزیع فرآورده.
- اطلاعات جمع آوری شده به طور صحیح، حفاظت شده و در زمان مناسب در اختیار کسب و کار طرح دیسپچینگ قرار گیرند.
- حفاظت از دارایی های طرح دیسپچینگ در برابر تهدیدات امنیتی که تمامیت، محرمانگی، دسترس پذیری و اعتبار طرح را به خطر می اندازند.
- اطمینان از اینکه تمام افرادی که در چرخه استحصال اطلاعات مشارکت دارند، از قوانین و اصول امنیت اطلاعات مطلع بوده و به آنها عمل می کنند.
- بهبود مداوم امنیت اطلاعات براساس فیدبک افرادی که در چرخه استحصال اطلاعات مشارکت دارند، رخدادهای و نتایج ممیزی ها
- اطمینان از رعایت سیاست های امنیت اطلاعات طرح دیسپچینگ و قوانین و احکام بالادستی شرکتی، دولتی و ملی.

## ۲ تعاریف

- ❖ **دارایی های طرح دیسپچینگ:** کامپیوتر دیسپچینگ مشتمل بر نرم افزارها، برد RTU، UPS، مانیتور، سیم کارت APN و اطلاعاتی که توسط این دارایی ها و کامپیوتر جمع اطلاعات در اتاق کنترل شرکت های توزیع فرآورده جمع آوری، پردازش و نگهداری می شوند.
- ❖ **ناظر طرح دیسپچینگ:** کسی یا کسانی که از سوی طرح دیسپچینگ شرکت ملی پخش به عنوان ناظر به شرکت های توزیع فرآورده معرفی می شوند.
- ❖ **افراد مجاز:**
  - در جایگاه: جایگاه دار و اپراتور جایگاه



نسخه ۱,۰  
۹۷/۷/۱۷

## طرح دیسپچینگ شرکت ملی پخش فرآورده های نفتی ایران - سیاست امنیت اطلاعات شرکت های توزیع فرآورده

➤ 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 شده اند.

### 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 جمع آوری، پردازش و ذخیره می شوند.

### 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 می شود 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.



طرح دیسپچینگ شرکت ملی  
پخش فرآورده‌های نفتی ایران -  
سیاست امنیت اطلاعات شرکت‌های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

- ✓ 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.
- هر نوع 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 شرکت‌های 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





طرح دیسپچینگ شرکت ملی  
پخش فرآورده‌های نفتی ایران -  
سیاست امنیت اطلاعات شرکت‌های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

- 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 متعاقباً 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 دارایی‌های دیسپچینگ در آن قرار دارد باشد (به عنوان مثال برای تعمیرات)، حتماً 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 Interface های Wifi، Infrared، Cellular، Bluetooth 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 سخت افزار

- پورتهای USB بسته باشند.
- امکان اتصال هیچ دستگاهی به سیستم وجود نداشته باشد. لازم است محدودیت ها (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 دارایی های دیسپچینگ ممنوع است.
- وجود رمز عبور برای ورود به Bios سیستم
- باید Bios بگونه ای 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 می باشد.
- 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 نرم افزار و سیستم عامل

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



طرح دیسپچینگ شرکت ملی  
بخش فرآورده‌های نفتی ایران -  
سیاست امنیت اطلاعات شرکت‌های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

- ✓ تمام سرویس‌های سیستم عامل که مشارکتی در عملکرد نرم‌افزار جایگاه سفید و نرم‌افزار تجمیع اطلاعات شرکت‌های 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 نرم‌افزارهای 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 اخلاقی 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 شرکت‌های توزیع فرآورده، هاست تجمیع اطلاعات است، Windows Server 2012 R2 باشد.
- ✓ نباید بر روی کامپیوتر دیسپچینگ و کامپیوتر یا سرور شرکت‌های توزیع فرآورده، بیش از یک سیستم عامل نصب باشد و از نرم‌افزارهایی 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.



طرح دیسپچینگ شرکت ملی  
پخش فرآورده های نفتی ایران -  
سیاست امنیت اطلاعات شرکت های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

- ✓ در صورت وجود داده های 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 نرم افزار جایگاه سفید بر روی کامپیوتر دیسپچینگ جایگاه نصب بوده و قابل استفاده باشد. نصب هر نرم افزار دیگری ممنوع است و باید این امر غیرفعال باشد (آنتی ویروس مشمول این بند نیست).
- ✓ تنها نرم افزارهای 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 نرم افزار دیگری ممنوع است و باید این امر غیرفعال باشد (آنتی ویروس مشمول این بند نیست).
- ✓ زمانی که از نرم افزار جایگاه سفید یا نرم افزار تجمیع داده دیسپچینگ استفاده نمی شود، باید سیستم عامل قفل شود.
- ✓ کد نرم افزار جایگاه سفید و یا نرم افزار تجمیع اطلاعات شرکت های توزیع فرآورده نباید قابل مشاهده و در دسترس باشد.
- ✓ اطلاعات استحصال شده توسط نرم افزار 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 نرم افزار تجمیع اطلاعات شرکت های توزیع فرآورده نباید تغییر کرده یا افشاء شوند.

➤ آنتی ویروس و وصله های 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 ویروس به صورت هفتگی یا حداقل دو هفته یک بار.
- ✓ وصله های امنیتی ماهی یکبار به صورت آفلاین توسط ادمین نصب شوند.
- ✓ تنها ادمین می تواند برای نصب وصله های امنیتی، بروز رسانی آنتی ویروس و بروز رسانی نرم افزار جایگاه سفید یا نرم افزار تجمیع اطلاعات شرکت های توزیع فرآورده، به طور موقت



طرح دیسپچینگ شرکت ملی  
بخش فرآورده‌های نفتی ایران -  
سیاست امنیت اطلاعات شرکت‌های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

و تا اتمام بروزرسانی، یک پورت USB را باز کند؛ پس از آن باید مجدداً 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 شرکت‌های 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 مجاز 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 شرکت‌های 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، الزاماً 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



طرح دیسپچینگ شرکت ملی  
پخش فرآورده های نفتی ایران -  
سیاست امنیت اطلاعات شرکت های  
توزیع فرآورده

نسخه ۱,۰  
۹۷/۷/۱۷

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

#### ۴,۶ کنترل تغییرات

- تغییرات، تعمیرات و هر نوع خطا یا اتفاق ای که رخ می دهد 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 دارایی های دیسپچینگ باید ابتدا از طرح دیسپچینگ شرکت ملی پخش مجوز گرفته شده و پس از انجام آن، صورتجلسه ای 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 سیاست ها هستند.



طرح دیسپچینگ شرکت ملی  
پخش فرآورده‌های نفتی ایران -  
سیاست امنیت اطلاعات شرکت‌های  
توزیع فرآورده

نسخه ۱،۰  
۹۷/۷/۱۷

## 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 شرکت‌های 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.



نسخه ۱،۰  
۹۷/۷/۱۷

طرح دیسپچینگ شرکت ملی  
پخش فرآورده های نفتی ایران -  
سیاست امنیت اطلاعات شرکت های  
توزیع فرآورده

### ۱۰،۳ عدم انطباق

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

### ۱۱ منابع

- سند سیاست های امنیت اطلاعات طرح دیسپچینگ
- سند جمع بندی مستندات احکام امنیتی حراست، افتا و پدافند غیرعامل

### ۱۲ تأییدیه ها

امضاء	تاریخ	نام و نام خانوادگی	سمت