

توافقنامه کاربری

اینجانب به شماره پرسنلی _____ حقوق دسترسی به **دارایی های اطلاعاتی** سازمانی که به من اعطاء (شده/خواهد شد) را درک کرده و (پذیرفته/می پذیرم)، همچنین نسبت به عواقب تخطی از دسترسی های اعطاء شده مخصوصاً هرگونه تلاش در جهت دسترسی به سرویس ها و دارایی هایی که مجوز آنها را ندارم و می تواند منجر به برخوردهای انضباطی گردد مطلع هستم. ضمناً می دانم و متعهد می گردم:

- از اینترنت و پست الکترونیکی شرکت تنها در جهت مسئولیت های اداری خویش استفاده نمایم.
- رویه گزارش دهی **رخدادها و نقاط ضعف امنیت اطلاعات** را پذیرفته و نسبت به آنها متعهد هستم.
- قبل از استفاده از هر دارایی اطلاعاتی حتما آموزش و آگاهی لازم نسبت به بهره برداری از آن دارایی را کسب نمایم.
- کوتاهی در تبعیت از این توافقنامه و یا هرگونه اقدام یا مشارکت در نقض امنیت اطلاعات سازمان می تواند منجر به برخورد بر اساس آیین نامه انضباطی سازمان با اینجانب گردد.

۱) کلمات عبور

- ۱-۱) کلمه عبور موقتی اولیه خود را در اولین ورود به سیستم تغییر خواهم داد.
- ۲-۱) کلمات عبوری را انتخاب می کنم که حداقل دارای ۶ کاراکتر طول و ترکیبی از اعداد و حروف باشند و چیزهایی که به سادگی قابل حدس زدن هستند مانند نام، تاریخ تولد، شماره تلفن و نباشند.
- ۳-۱) کلمه عبور خود را تحت هیچ شرایطی افشاء نمی کنم و یا با دیگران به اشتراک نمی گذارم. همچنین کلمه عبور خود را به هیچ عنوان در جایی ثبت نمی کنم مگر مجوز چنین کاری را از مدیر فناوری اطلاعات کسب کرده باشم.
- ۴-۱) کلمه عبور خود را در فرایند خودکار ورود (Log on) ذخیره نمی کنم.
- ۵-۱) کلمه عبور خود را در فواصل زمانی تعیین شده توسط سازمان تغییر می دهم و تلاشی در راستای استفاده مجدد از کلمات عبور قبلی یا کلمات عبور جدید ولی شبیه کلمات عبور قبلی نمی کنم. همچنین در صورت مشاهده مدارکی دال بر احتمال سوء استفاده از کلمه عبور فعلی زودتر از موعد مقرر اقدام به تغییر کلمه عبور می نمایم.
- ۶-۱) کلمات عبور یکسان برای استفاده های کاری و شخصی بکار نمی گیرم.

۲) خط مشی میز پاک، محافظ صفحه نمایش (Screen Savers) و باز تولید اطلاعات

- ۱-۲) می دانم که ملزم به حصول اطمینان از این امر هستم که هیچگونه اطلاعات محرمانه یا خیلی محرمانه (بصورت کاغذی یا در قالب رسانه های ذخیره سازی قابل حمل) نباید روی میز، در اطراف میز، یا نزدیک تجهیزات باز تولید اطلاعات (دستگاه های کپی، فاکس، اسکنر) در زمانیکه حضور ندارم رها باشد.

۲-۲) می‌دانم که ملزم به حصول اطمینان از این امر هستم که هیچکس نمی‌تواند به سیستم کامپیوتری من در زمان عدم حضور من دسترسی پیدا کند و از اینرو باید از محافظ صفحه نمایش دارای کلمه عبور (که در صورت عدم فعالیت در ۵ دقیقه فعال می‌شود) استفاده نمایم و یا اینکه در زمان ترک سیستم باید آنرا فعال نمایم. (بر اساس راهنمای کاربردی امنیت اطلاعات)

۳-۲) می‌دانم که ملزم به پایان دادن و بستن جلسات (Sessions) کامپیوتری فعال (بستن پنجره های باز برنامه ها و اینترنت) زمانی که کارم با آنها تمام شده هستم و ملزم به خروج (Log off) از سیستم در پایان کارم هستم و نه اینکه فقط صفحه مانیتور را خاموش کنم.

۴-۲) می‌پذیرم که نباید رسانه‌های ذخیره‌سازی شخصی، MP3 Player ها، دوربین‌های دیجیتالی و را با خود به محل کار آورده و از آنها استفاده نمایم.

۵-۲) می‌پذیرم که فقط می‌توانم از تجهیزات بازتولید اطلاعات (دستگاه‌های کپی، فاکس، اسکنر) برای مقاصد سازمانی مجوز گرفته شده استفاده نمایم. همچنین اطمینان می‌دهم که از تجهیزات و دستگاه‌هایی که متناسب با دسترسی اینجانب است استفاده نمایم.

۳) نرم افزار

۱-۳) اطمینان می‌دهم که هیچگونه تلاشی به منظور غیرفعال‌سازی یا لغو هیچیک از نرم‌افزارهای نصب شده سازمانی شامل نرم‌افزار آنتی ویروس، فایروال‌ها و سرویس‌های به‌روزرسانی خودکار به انجام نرسانم.

۲-۳) می‌پذیرم که هیچ نرم‌افزاری را بر روی کامپیوتر خود و یا دیگر تجهیزات نصب نمی‌کنم مگر آنکه مجوز سازمانی آن از قبل صادر شده باشد و یا مدیر فناوری اطلاعات مجوز آن را ارائه کرده باشد.

۴) کنترل داده‌ها و اطلاعات

۱-۴) اطمینان می‌دهم که به الزامات قانونی در رابطه با استفاده از کامپیوتر خود شامل مقررات حفاظت از داده‌ها و اطلاعات و نیز حریم خصوصی پایبند هستم.

۵) پشتیبان‌گیری و طبقه‌بندی اطلاعات

۱-۵) تأیید می‌نمایم که اینجانب مسئول حصول اطمینان از این امر هستم که تمامی اطلاعات موجود بر روی کامپیوتر تحویلی اینجانب به درستی از نظر اهمیت و محرمانگی طبقه‌بندی و شناسایی شده‌اند.

۲-۵) تأیید می‌نمایم که مسئول پشتیبان‌گیری از اطلاعات موجود بر روی سیستم خود و فضاهاى مجازى مشترك اختصاص یافته توسط سازمان هستم. می‌دانم که ملزم به ذخیره‌سازی تمام داده‌ها و اطلاعات در دایرکتوری مشخص (به غیر از درایو C کامپیوتر خود) می‌باشم.

٦) نگهداری

می‌پذیرم که مسئول امنیت فیزیکی دستگاه کامپیوتر خود هستم و هرگونه نقص در آن را فوراً و مطابق رویه گزارش‌دهی رخداده‌ها و نقاط ضعف (طبق فرم شماره ۸۹) گزارش می‌کنم.

٧) ممیزی و نظارت امنیتی

می‌دانم که بصورت منظم و یا نامنظم و بر اساس رویه ممیزی داخلی و دیگر رویه‌های سازمانی مورد ممیزی و نظارت امنیتی قرار می‌گیرم.

٨) ابطال و تغییر حقوق دسترسی

می‌دانم پس از هرگونه جابجایی فیزیکی و سازمانی لازم است حقوق دسترسی اینجانب ابطال و یا تغییر یابد لذا در صورت مشاهده هرگونه مغایرت، ملزم به اعلام موضوع به مدیریت فناوری اطلاعات می‌باشم.

تاریخ: امضاء:

* توضیحات

- دارایی اطلاعاتی به هر موجودیتی اطلاق می‌شود که برای شرکت دارای ارزش باشد.
- رخداد امنیت اطلاعات یک یا مجموعه‌ای از رویدادهای ناخواسته و یا پیش‌بینی نشده است که به احتمال زیاد عملیات کسب و کار را به خطر انداخته و امنیت اطلاعات را تهدید می‌کند.
- فرم گزارش رخداد/نقطه ضعف امنیتی به شماره ۸۹ در پرتال داخلی شرکت (در DMS منوی دریافت/فرم‌های داخلی) موجود می‌باشد.
- نام کاربری و کلمه عبور هر کاربر مطابق با رویه مجوزدهی شرکت، صادر می‌شود.