برگه راهنمایی نکات امنیت داده در حوزه مدیریت عملیاتی داده‌ها
آپریل ۲۰۲۲

ضمن تشکر و قدردانی از حمایت های CLEAR Global و وزارت اروپا و امور خارجه فرانسه، ترجمه ی این برگه راهنما با کمک CartONG انجام شده.

مقدمه
امنیت داده بخشی کلیدی و مهم در زمینه مسئولیت‌پذیری در قبال داده‌ها می‌باشد: مدیریت امن، اخلاقی و موثر داده‌ها برای پاسخ عملیاتی. این خود مستلزم مجموعه‌ای از تدابیر فیزیکی، فناوری و اقداماتی میباشد که از محرمانه بودن و سالم بودن داده‌ها و دسترسی به آنها حفاظت می‌کند، و از زیان، از دست رفتن، تغییر، به دست آوردن یا فاش کردن تصادفی یا عمدی، غیرقانونی یا غیرمجاز آن جلوگیری می‌کند.

این برگه راهنما مجموعه‌ای از اقدامات توصیه شده در زمینه مدیریت عملیاتی داده‌ها جهت حفظ امنیت داده را گردآوری کرده‌است. این اقدامات باید مطابق با دستورالعمل‌های مؤسسات، سیاست‌های مرتبط با آنها و چارچوب‌های قانونی و نظارتی‌شان اجرا شوند.

اجرای مدیریت مناسب رمزهای عبور
- دستگاه‌ها و حساب‌های خود را با رمزهای عبور قوی که شامل اعداد، حروف بزرگ و کوچک، و نمادهایی با حداقل ۱۶ کاراکتر در هر رمز عبور هستند ایمن کنید.
- برای تمامی حساب‌ها، احراز هویت چندعاملی را فعال کنید.
- از استفاده مجدد یک رمز عبور برای حساب‌های مختلف خود خودداری کنید.
- از ذخیره رمزهای عبور خود به صورت فیزیکی (مانند یادداشت) یا دیجیتالی (در فایلی روی دستگاه تان) خودداری کنید و رمز عبور خود را با دیگران به اشتراک نگذارید.
- قابلیت "مرا به خاطر بسپار" را در برنامه‌ها و مرورگرها فعال نکنید.
- در صورت گم شدن یا سرقت دستگاه خود، بلافاصله رمزهای عبور حساب‌های آنلاین خود را تغییر دهید.

از نرم‌افزارهای ضد ویروس/ضد بدافزار استفاده کنید
- مطمئن شوید که در دستگاه‌های خود، نرم‌افزارهای ضد ویروس/ضد بدافزار مناسب نصب شده باشد.
- اگر سوالی درباره ابزارهای مناسب یا نحوه پیکربندی آن‌ها دارید، با کارشناس فناوری اطلاعات دفتر خود مشورت کنید.

نرم‌افزارها و سیستم‌عامل‌ها را آپدیت و به‌روز نگه دارید
- با دقت بررسی کنید که دستگاه، نرم‌افزارها، برنامه‌ها و پلاگین‌های مرورگر شما به‌روز هستند و به‌روزرسانی‌های خودکار را برای سیستم‌عامل خود فعال نگه دارید.
- از مرورگرهای وبی مانند Chrome یا Firefox استفاده کنید که به‌روزرسانی‌های امنیتی خودکار دریافت می‌کنند.
- در پایان روز، دستگاه‌ها را خاموش کنید تا به‌روزرسانی‌ها انجام شوند و در برابر حملات از آنها محافظت شود.

به حملات فیشینگ آگاه باشید، از آنها دوری کرده و به دقت کلیک کنید
- در زمان دریافت ایمیل‌ها یا پیام‌های مشکوک، آدرس/اطلاعات تماس فرستنده را بررسی کرده و فقط زمانی بر روی لینک‌ها یا پیوست‌ها کلیک کنید که به فرستنده آنها اعتماد دارید.
- به ایمیل‌های مشکوک پاسخ ندهید و آن‌ها را برای همکاران خود ارسال نکنید.
- هر فعالیت مشکوکی را گزارش کنید به تیم پشتیبانی فناوری اطلاعات خود.

از دستگاه های تلفن همراه مسئولانه و به درستی استفاده کنید

- **در صورت امکان، از دستگاه‌های جداگانه برای اهداف کاری متفاوت استفاده کنید. همواره دستگاه‌های کاری خود را در مکانی امن نگه دارید و از جابجایی بی‌مورد آن‌ها اجتناب کنید.**
- **از ابزارهای پیام‌رسانی تأیید شده توسط سازمان خود استفاده کنید که امکان رمزگذاری انتها به انتها در آنها فراهم شده باشد.**
- **در صورت امکان، اتصال بلوتوث را خاموش نگه دارید و استفاده از آن را به حداقل برسانید.**
- **زمانی که آنلاین مشغول انجام کارهایتان هستید، از یک شبکهٔ خصوصی مجازی (VPN) تأیید شده توسط سازمان خود استفاده کنید. اگر از دستگاه یا کامپیوتر عمومی استفاده می‌کنید، همواره از حساب‌های خود خارج شوید.**
- **قابلیت‌های "بازگشاییِ قفلِ بیومتریک" را غیرفعال کنید - به خصوص زمانی که در حال حرکت هستید.**

در حفظ اطلاعات حساس بکوشید و تا حد امکان سعی کنید مقدار آنها را به حداقل کاهش دهید

- **یک سیستم ثبت داده در دسترس داشته باشید که سطح حساسیت هر نوع داده‌ای را که توسط دفتر شما مدیریت می‌شود نشان دهد.**
  سطوح حساسیت را به صورت منظم بررسی کنید تا با تغییرات محیط و شرایط، همزمان به‌روزرسانی شوند.
- **برای دستیابی به اهداف فعالیتی مرتبط با مدیریت داده، فقط حداقل داده ی مورد نیاز را گردآوری کنید.**
- **اطلاعات حساس را تنها تا زمان تحقق هدفی که برای آن مدیریت می‌شوند و طبق راهنماها، قوانین و مقررات مربوطه نگهداری کنید.**
- **برای انتقال و ذخیره سازی داده ها از ابزارها و راه های ارتباطی که توسط سازمان شما تأیید شده‌اند استفاده کنید (بر روی سرور لوکال سازمان، کامپیوتر یا لپتاپ شرکت؛ یا به کمک سرورها و سیستم‌های از راه دور به وسیله ی برنامه‌هایی مانند OneDrive، SharePoint و Teams).**
- **از فایل‌های حاوی اطلاعات حساس (Word، Excel، PDF) به وسیله رمز عبور محافظت کنید و رمز عبور سند را از راه‌های ارتباطی جداگانه به اشتراک بگذارید (به عنوان مثال، رمز عبور سندی که با ایمیل ارسال شده را از طریق پیامک به اشتراک بگذارید).**
- **تعداد افرادی که به داده‌های حساس دسترسی دارند را محدود کنید و با دقت آنها را نظارت کنید.**
- برای تمامی داده‌های تحت مدیریت، یک برنامه زمان‌بندی جهت نگهداری و از بین بردنشان تعریف کنید و از ابزارهای مناسب برای از بین بردن آنها استفاده کنید.
- متن پیام های ایمیل خود را رمزگذاری کنید.

منابع کلیدی

- راهنمای عملیاتی IASC در مورد مسئولیت پذیری در قبال اطلاعات و داده ها در اقدام بشردوستانه
- یادداشت راهنما در مورد مدیریت حوادث اطلاعات و داده ها
- برگه راهنمایی در مورد استفاده مسئولانه ودرست از ابزارهای برگزاری آنلاین کنفرانس

برای اطلاعات بیشتر در مورد مدیریت داده‌های حساس در اقدامات بشردوستانه، از صفحه مسئولیت‌پذیری در قبال داده‌ها در وب سایت سنتر دیدن کنید یا با تیم ما به آدرس centrehumdata@un.org در تماس باشید.