

ممنوعیت جلوگیری از دسترسی کاربران مجاز به داده و سامانه

ماده ۱۰ قانون جرایم رایانه‌ای، جلوگیری غیرمجاز از دسترسی اشخاص مجاز به داده‌ها یا سامانه‌ها را با اقداماتی مانند پنهان کردن داده، تغییر گذرواژه یا رمزنگاری موضوع جرم‌انگاری قرار می‌دهد. در این مقرر، محروم شدن دارنده حق دسترسی از استفاده مجاز اهمیت دارد.

این موضوع در تحویل پروژه، پایان همکاری مدیر شبکه و اختلاف میان کارفرما و پیمانکار اهمیت عملی پیدا می‌کند. وجود اختلاف قراردادی به‌تنهایی مجوز مسدودسازی خودسرانه دسترسی نیست و حدود اختیارات و تعهدات باید بر اساس قرارداد و قانون بررسی شوند.

به‌عنوان توصیه مدیریتی، حساب‌های حیاتی و روش‌های بازیابی بهتر است تحت کنترل سازمان و با مسئولیت مشخص نگهداری شوند. مستندسازی تحویل دسترسی‌ها و طراحی حساب اضطراری کنترل‌شده می‌تواند وابستگی کامل به یک فرد را کاهش دهد.

تغییر رمز یا رمزنگاری برای حفاظت مشروع، با جلوگیری غیرمجاز از دسترسی یکسان نیست. هدف، اختیار و نتیجه اقدام باید بررسی شوند؛ توصیه‌های این متن برای کاهش ریسک عملیاتی‌اند و درباره یک پرونده یا اختلاف مشخص حکم قطعی صادر نمی‌کنند.

مبنای قانونی: ماده ۱۰ قانون جرایم رایانه‌ای. مشاهده متن قانون. این مطلب خلاصه آموزشی است، نه متن رسمی قانون یا مشاوره حقوقی؛ برای اقدام حقوقی باید متن معتبر و اصلاحات لازم‌الاجرا بررسی شود.