نظام‌نامه یکپارچه مدیریت امنیت اطلاعات و دارایی‌های فیزیکی/دیجیتال

(بر اساس استاندارد ۲۷۰۰۱)

گرد آوری شده توسط مشاورین شرکت مهندسی پردازش ساختارهای بازتهران OSP

ویرایش اول: نهم اردیبهشت ماه ۱۴۰۵

۱. حاکمیت و سازماندهی امنیت

- تعیین دارایی‌ها : کلیه دارایی‌های فیزیکی (PLCها، سرورها) و دارایی‌های اطلاعاتی (نقشه‌های فنی، فرمول‌های اختلاط) باید دارای «مالک مشخص» و طبقه‌بندی محرمانگی (محرمانه، داخلی، عمومی) باشند.

- مدیریت ریسک: هر واحد موظف است سالانه «ارزیابی ریسک عملیاتی» انجام داده و برای ریسک‌های با سطح بالا (مانند توقف خط تولید بر اثر باج‌افزار)، طرح مقابله ارائه دهد.

۲. کنترل‌های دسترسی و هویت

- اصل حداقل دسترسی: دسترسی به نرم‌افزارهای حساس مانند سیستم بارگیرخانه یا تنظیمات کوره، فقط باید در حد نیاز شغلی تخصیص یابد.

- احراز هویت چندعاملی: برای تمامی دسترسی‌های راه دور و ورود به سامانه‌های مالی وERP، استفاده از رمز یکبار مصرف الزامی است.

۳. امنیت فیزیکی و محیطی

- مناطق امن: اتاق سرور، اتاق فرمان، پست‌های برق و آزمایشگاه X-Ray به عنوان «مناطق تحت نظارت» تعریف شده و ورود/خروج باید با کارت تردد ثبت و توسط دوربین‌های VMS مانیتور شود.

- امنیت تجهیزات: تجهیزات فنی نباید بدون مجوز کتبی از سایت خارج شوند و پورت‌های بلااستفاده روی سوئیچ‌های صنعتی باید مسدود گردند.

۴. امنیت عملیات و ارتباطات

- ایزولاسیون شبکه: جداسازی کامل شبکه IT (اداری) از شبکه OT (تولید) از طریق Firewall های لایه ۷ جهت جلوگیری از انتقال آلودگی بدافزاری از سیستم‌های اداری به بخش تولید.

- پشتیبان‌گیری: اجرای پروتکل پشتیبان‌گیری منظم و تست دوره‌ای صحت بازیابی برای اطمینان از تداوم تولید.

۵. امنیت در چرخه حیات تجهیزات و تأمین‌کنندگان

- امنیت در زنجیره تأمین: کلیه پیمانکاران (اعم از پیمانکاران نسوزکاری یاIT) ملزم به امضای توافق‌نامه عدم افشا (NDA) و رعایت الزامات امنیتی OSP در هنگام حضور در سایت هستند.

- توسعه امن: هرگونه تغییر در کدنویسیPLC ها یا نرم‌افزارهای داخلی باید ابتدا در محیط تست بررسی و سپس وارد محیط عملیاتی شود.

۶. مدیریت حوادث و تداوم کسب‌وکار (BCM)

- گزارش‌دهی وقایع: کلیه کارکنان موظفند هرگونه اختلال مشکوک در سیستم‌ها (حتی کندی غیرعادی سیستم باسکول) را فوراً به واحدIT/ حراست گزارش کنند.

- برنامه تداوم کسب‌وکار: تدوین دستورالعمل‌های جایگزین برای زمان قطع دسترسی به ERP یا سیستم‌های اتوماسیون صنعتی جهت جلوگیری از توقف فروش و صادرات.

۷. انطباق و ممیزی

ممیزی داخلی: تیم ممیزی دارای صلاحیت موظف است هر ۶ ماه یکبار تطابق عملکرد واحدها با این دستورالعمل را ممیزی کرده و عدم‌انطباق‌ها را جهت اصلاح ابلاغ نماید.