دستورالعمل اقدام‌های اضطراری دستگاه‌ها

به‌منظور ایجاد آمادگی جهت مقابله با تهدیدهای احتمالی، دستگاه‌های اجرایی مکلف هستند اقدام‌های ذیل را در کوتاه‌ترین زمان ممکن، انجام دهند:

۱. قطع دسترسی‌های از راه دور (اعم از دسترسی‌های مدیریتی و کاربری) به کلیه سامانه‌ها و خدمات
۲. حذف حساب‌های کاربری غیرضروری و بلااستفاده در سامانه‌ها و شبکه دستگاه
۳. تغییر کلمات عبور کلیه کاربران در کلیه سامانه‌ها و خدمات، به‌صورت متمرکز و توسط مدیر شبکه
٤. قطع اتصال سامانه‌های اداری (پرسنلی، حضور و غیاب، اتوماسیون اداری و ...) و شبکه داخلی دستگاه، از شبکه اینترنت
٥. تأمین مسیر دوم جهت اتصال سامانه‌ها و خدمات عمومی دستگاه به شبکه اینترنت (برای ستاد وزارتخانه‌ها و سایر دستگاه‌های کلیدی)
٦. تعیین و در دسترس بودن نماینده دستگاه به‌صورت شبانه‌روزی (۲۴*۷) جهت همکاری با مرکز ماهر
۷. در دسترس قرار داشتن آخرین نسخه از اطلاعات دارایی‌های فناوری اطلاعات دستگاه (اطلاعات ساختار، تجهیزات و خدمات شبکه و مسئول مدیریت/پشتیبانی هر یک از آن‌ها)
۸. محدود نمودن دسترسی کاربران به خدماتی که کاربر خارج از کشور ندارند، صرفاً به دسترسی از طریق شبکه IP داخل کشور (ایران اکسس نمودن)
۹. تهیه نسخه پشتیبان از نرم‌افزارها و اطلاعات شبکه و انجام حداقل یک مرتبه آزمون صحت نسخه پشتیبان
۱۰. راه‌اندازی نسخه افزونه سامانه‌های اطلاعاتی کلیدی دستگاه به‌صورت Active Standby، به‌نحوی که در صورت وقوع حادثه و از دسترس خارج شدن آن سامانه، نسخه افزونه بلافاصله قابلیت جایگزینی داشته باشد
۱۱. عدم عملیاتی نمودن سامانه اطلاعاتی و ارائه خدمت جدید، قبل از انجام ارزیابی امنیتی و رفع آسیب‌پذیری‌های احتمالی
۱۲. به‌روز رسانی تمامی نرم‌افزارها و میان‌افزارهای تجهیزات شبکه و امنیت
۱۳. رفع آسیب‌پذیری‌های شناخته‌شده (ثبت‌شده در پایگاه‌های داده آسیب‌پذیری بین‌المللی) سامانه‌های اطلاعاتی و شبکه دستگاه
۱٤. رفع آسیب‌پذیری‌های اعلام‌شده توسط مرکز ماهر به دستگاه‌ها
۱٥. اعلام هرگونه رفتار مشکوک در شبکه، کاربران و سامانه‌ها به مرکز ماهر (شماره تلفن ۰۲۱-۸۸۱۱۵۷۲۴ یا آدرس پست الکترونیکی Report@Cert.ir)
۱٦. آمادگی رسیدگی به حوادث احتمالی و همکاری با تیم رسیدگی به حادثه مرکز ماهر جهت:
- هماهنگی حضور تیم رسیدگی به حادثه مرکز ماهر در محل دستگاه
- اعطای فوری کلیه دسترسی‌های کاربری و مدیریتی لازم به این تیم، جهت انجام عملیات فارنزیکس