پیوست ۲

الزامات امنیتی در خصوص زیرساخت‌های برگزاری مجامع الکترونیکی

۱- آزمون نفوذپذیری برنامه کاربردی توسط حداقل یک شرکت تخصصی دارای پروانه معتبر از مدیریت راهبردی افتا و دریافت گواهینامه امنیتی برنامه کاربردی از شرکت مذکور

۲- ارزیابی امن سازی تجهیزات زیرساخت، سیستم‌عامل‌هاو سرویس‌ها توسط حداقل یک شرکت تخصصی دارای پروانه معتبر از مدیریت راهبردی افتا و دریافت گواهینامه امن‌سازی از شرکت مذکور

۳- وجود مستند معماری استقرار سامانه

۴- وجود طرح منطقی و فیزیکی مستند استقرار شبکه

۵- رعایت کدنویسی امن بر اساس آخرین استانداردها، مراجع و اصول امنیتی مانند OWASP

۶- عدم استفاده از وب‌سایت‌های آماده متن‌باز

۷- انتقال داده‌های محرمانه بر روی بسترهای ارتباطی با استفاده از پروتکل‌های امن و به صورت رمز شده

۸- ذخیره داده‌های محرمانه به صورت رمز شده (در پایگاه داده، لاگ و ...) با استفاده از الگوریتم‌ها، توابع رمزنگاری و درهم‌سازی قوی

۹- ذخیره سازی رای سهامداران به صورت محرمانه

۱۰- جداسازی سیستم‌عامل برنامه کاربردی از پایگاه داده

۱۱- اعمال امن‌سازی در سطوح مختلف (تجهیزات شبکه و امنیت، سیستم‌عامل، وب‌سرور و پایگاه داده)

۱۲- به‌روزرسانی سیستم‌عامل‌ها و مولفه‌های نصب شده بر روی آن‌ها و اعمال وصله‌های امنیتی

۱۳- نصب آنتی‌ویروس با قابلیت مدیریت متمرکز بر روی سیستم‌عامل‌ها و بروزرسانی آن

۱۴- رعایت الزامات ثبت لاگ (نسخه ۲) و بخش ۹ الزامات امنیت مرکز نظارت بر امنیت اطلاعات بازار سرمایه

۱۵- پشتیبان‌گیری از داده‌های مهم و پیکربندی سرویس‌ها و تجهیزات

۱۶- تضمین دسترس‌پذیری سامانه با رعایت افزونگی در سطوح مختلف

۱۷- انجام load test و stress test قبل از عملیاتی شدن سامانه و حصول اطمینان از تحمل بار در زمان رای گیری

۱۸- عبور ترافیک بین کاربر نهایی و سرویس عملیاتی از فایروال (با رعایت اصل حداقل دسترسی) و IPS با تنظیمات صحیح(به گونه‌ای که از حملات سایبری جلوگیری نماید)

۱۹- حفاظت از برنامه کاربردی توسط تجهیزWAF با تنظیمات صحیح (به گونه‌ای که از حملات سایبری جلوگیری نماید)

۲۰- تمامی ارتباطات شبکه‌ای نقطه به نقطه امن با استفاده از رمزنگاری با سایر شرکت‌ها و سازمان‌ها جهت دریافت اطلاعات

۲۱- تفکیک زون‌های شبکه بر اساس سطوح حساسیت امنیتی و ماهیت کاری (تفکیک زون پایگاه داده، زون برنامه کاربردی، زون مدیریت و ...)

۲۲- عدم وجود دسترسی سرورها به اینترنت

۲۳- به‌روزرسانی تجهیزات شبکه و امنیت به صورت مداوم

۲۴- عدم وجود دسترسی مستقیم به درگاه‌های پیکربندی و پنل‌های مدیریتی تجهیزات، سرورها و سامانه از طریق اینترنت عمومی