نکات عمومی امنیت در سامانه‌های معاملات برخط و سامانه‌های صدور و ابطال الکترونیکی واحدهای صندوق‌های سرمایه‌گذاری

ردیف	عنوان	توضیحات
۱	**الزام به تغییر کلمه عبور کاربر در اولین ورود**	زمانی که کاربری برای اولین بار به سامانه وارد می‌شود، باید با صفحه تغییر رمز عبور مواجه شود.
۲	**الزام به تغییر دوره‌ای کلمه عبور کاربر**	از آخرین زمانی که یک کاربر رمز عبور خود را تغییر داده است، باید به صورت دوره ای (حداکثر ۳ ماه)، به محض ورود به سامانه و تا زمانی که رمز را تغییر نداده است، ۱. یا با صفحه تغییر رمز مواجه شود. ۲. یا پیام هشداری برای وی ظاهر شود که کاربر گرامی، با توجه به گذشت (مثلا ۳ ماه) از آخرین تغییر رمز عبور، لطفا از طریق (....) اقدام به تغییر رمز عبور خود فرمایید.
۳	**نمایش میزان استحکام رمز عبور در حین تایپ کاربر**	در تمام بخش‌های تغییر یا تعیین رمز عبور در سامانه‌ها، باید در حین تایپ رمز، قدرت امنیتی رمز به کاربر نمایش داده شود تا بتواند درکی از میزان استحکام رمز انتخابی خود داشته باشد. لازم به ذکر است، قدرت رمزهای عبور به صورت زیر می‌تواند تقسیم بندی شود: ۱. **ضعیف**: کمتر از ۸ حرف باشد یا تنها از یک نوع کاراکتر (مثلا فقط عددی، یا فقط حرف کوچک، یا فقط حرف بزرگ) استفاده شده باشد. ۲. **متوسط**: ضعیف نباشد و تنها از دو نوع کارکتر استفاده شده باشد (مثلا فقط حرف کوچک و عدد) ۳. **قوی**: متوسط نباشد و حداقل از سه نوع کاراکتر استفاده شده باشد. (مثلا حروف کوچک، بزرگ و رقم) در صورتی که رمز عبور وارد شده توسط کاربر در دسته بندی "ضعیف" قرار گیرد، نباید سیستم آن را بپذیرد.
۳	**لزوم وجود صفحه کلید مجازی در صفحه ورود**	ضروری است قابلیت ورود نام کاربری و کلمه عبور کاربر در صفحه ورود سامانه با استفاده از صفحه کلید مجازی نیز برای کاربر مهیا باشد.
۴	**لزوم اطلاع‌رسانی نکات امنیتی در صفحه ورود**	با توجه به ضرورت آگاهی بخشی عمومی در خصوص امنیت اطلاعات، ضروری است نکات امنیتی شامل موارد ذیل در صفحه ورود به سامانه درج گردد:

		• سامانه [نام سامانه+ نام شرکت] با استفاده از پروتکل امن SSL به مشتریان خود ارائه خدمت نموده و با آدرس https://[Website-URL] شروع می‌شود. لطفا پیش از ورود هرگونه اطلاعات، آدرس موجود در بخش مرورگر وب خود را با آدرس فوق مقایسه نمایید و درصورت مشاهده هر نوع مغایرت احتمالی، از ادامه کار منصرف شده و موضوع را با ما در میان بگذارید. • برای حفاظت از اطلاعات حساب کاربری خود، حتی المقدور از صفحه کلید مجازی استفاده نمایید. • هرگز اطلاعات حساب کاربری (نام کاربری و رمز عبور) خود را در اختیار دیگران قرار ندهید. • پس از اتمام کار با سامانه، حتما بر روی دکمه خروج از سامانه کلیک نمایید. • {نکات امنیتی صحیح بیشتر نیز می تواند توسط شرکت افزوده شود.} توجه شود که این نکات، باید به شیوه‌ای ساده در اختیار کاربر قرار گیرد.
۵	**لزوم ثبت فعالیت ورود و خروج کاربر به سامانه**	در راستای آگاهی کاربران از ورودهای مشکوک به حساب کاربری آن‌ها در سامانه ضروری است هر گونه فعالیت ورود و خروج کاربر به سامانه بر اساس آدرس IP و زمان ورود و خروج ثبت گردیده و برای کاربر، قابل مشاهده و گزارش‌گیری باشد. اطلاعات فوق برای کاربردهای احتمالی فارنزیکس و ردگیری جرائم، باید در سمت سرور، حداقل برای مدت شش ماه نگهداری شود.
۶	**حذف Data Caching در مرورگر**	در راستای عدم افشای اطلاعات کاربری ضروری است امکان Caching داده‌ها (به خصوص داده‌های شخصی و محرمانه کاربران) توسط مرورگر، غیر فعال گردد.[1] علاوه بر این، برای فیلدهای ورودی حساس همچون فرم لاگین یا فرم ثبت سفارش خرید و فروش، امکان Autocomplete باید غیرفعال گردد تا مرورگر اطلاعات حساب کاربری را Cache نکند.
۷	**وجود دکمه خروج از سامانه به صورت واضح و**	دکمه خروج از سامانه، باید به صورت واضح در تمام صفحات سامانه (پس از ورود کاربر) قابل مشاهده و در دسترس باشد. وجود دکمه خروج در زیرمنوها صحیح نیست. همچنین

[1] راهنما: در این خصوص می‌توان از سرایندهای HTTP جهت کنترل Cache (Cache Control HTTP Headers) و یا متا تگ‌های درون صفحه HTTP استفاده کرد.

	همه جا در دسترس	توصیه می‌شود در صورتی که از یک آیکن برای دکمه خروج استفاده شده است، حتما کنار آن، عبارت خروج قید گردد.