**با سلام و احترام**

**به استحضار می‌رساند، با توجه به ابلاغ الزامات امنیتی در خصوص مدیریت نام‌های کاربری و گذرواژه، از طرف مرکز مدیریت راهبردی افتا، سیاست‌های گذرواژه‌های قوی، بازیابی گذرواژه و حفاظت از گذرواژه اعلام شده، به شرح زیر ارسال می‌گردد .**

**سیاست‌های تعیین گذرواژه‌های قوی**

کاربران در هنگام تعیین گذرواژه برای نام کاربری خود در شبکه یا سامانه‌های دانشگاه، نکات زیر را رعایت نمایند:

- برای کاربران عادی یک گذرواژه حداقل باید ۸ کاراکتر و برای مدیران حداقل ۱۳ کاراکتر باشد.
- گذرواژه‌های کاربران نباید بر اساس اطلاعات شخصی مانند نام همسر، تاریخ تولد، شماره تلفن همراه و غیره باشد که به راحتی بتوان آن را حدس زد یا به آن دسترسی داشت.
- گذرواژه‌های کاربران نباید کلمه‌ای از یک زبان، لغت‌نامه، زبان عامیانه، لهجه، گویش و غیره مانند password، ۱۲۳۴۵۶۷۸۹ ، qwerty و غیره باشد.
- گذرواژه بایستی ترکیبی از حروف الفبا و اعداد باشدکه در آن از حروف بزرگ، حروف کوچک، اعداد و علامت‌هایی مانند* و % و $و # و کاراکتر space استفاده شده است.
- گذرواژه‌های کاربران باید محرمانه نگه داشته شود و نباید به اشتراک گذاشته شده یا در جایی پست شود یا به هر نوعی افشا گردد (به عنوان مثال بر روی میز کار قرار داده نشود.)

**سیاست‌های حفاظت از گذرواژه**

- از انتقال گذرواژه‌ها به طرق مختلف مانند تلفن، ایمیل و اینترنت و مطرح کردن در حضور دیگران اجتناب شود.
- فرمت مرسوم انتخاب گذرواژه‌ها، با دیگران مطرح نگردد.
- از ذخیره‌سازی گذرواژه‌ها به صورت رمز شده یا متن آشکار در قالب فایل‌های اکسل یا متنی اجتناب گردد.
- گزینه "گذرواژه را به خاطر بسپار" در مرورگر و برنامه‌های کاربری فعال نگردد.
- در صورت احتمال افشای گذرواژه، فوراً نسبت به تغییر آن اقدام شود.
- قبل از ترک میز کار، حساب کاربری قفل گردد.

**سیاست‌های بازیابی گذرواژه**

- بازیابی گذرواژه کاربر، فقط زمانی که توسط کاربر درخواست می‌شود و پس از راستی آزمایی هویت انجام می‌شود.
- پس از ۵ دقیقه عدم فعالیت، حساب کاربری قفل شده و کاربر ملزم به ورود مجدد گذرواژه می‌شود.