سازمان نظام مهندسی
ساختمان خراسان رضوی

آیین نامه تخلفات رایانه ای

سازمان نظام مهندسی ساختمان خراسان رضوی

تاریخ تصویب : ۹۰/۰٤/۲۳

آیین نامه تخلفات رایانه‌ای سازمان نظام مهندسی ساختمان خراسان رضوی

مقدمه

این آیین‌نامه به منظور مشخص ساختن نحوه برخورد با تخلفات رایانه‌ای و نیز اتخاذ تدابیری برای پیشگیری از آن، در جلسه مورخ ۹۰/۰۴/۲۳ هیئت رئیسه سازمان به تصویب رسیده است و پس از ابلاغ برای کلیه واحدها لازم‌الاجرا خواهد بود.

فصل اول – تعاریف، حوزه تسری

ماده ۱.برخی از واژه‌ها و عبارات مورد استفاده به شرح زیر تعریف می‌شود:

۱-۱.سازمان: سازمان نظام مهندسی ساختمان خراسان رضوی

۱-۲.هیئت رئیسه: هیئت رئیسه سازمان نظام مهندسی ساختمان خراسان رضوی

۱-۳.مرکز رایانه: واحد فناوری اطلاعات و ارتباطات سازمان

۱-۴.مراجع رسیدگی به تخلفات رایانه‌ای: هیئت رئیسه

۱-۵.مسئول امور رایانه سازمان: شخصی که از سوی ریاست سازمان جهت مدیریت امورراینه‌ای منصوب می‌گردد.

۱-۶.کارشناس رایانه سازمان: شخص یا اشخاصی که جهت ارایه خدمات رایانه‌ای منصوب می‌گردد.

۱-۷.متصدی امور رایانه: عنوانی مشترک برای مسئول امور رایانه و نیز هر کدام از کارکنان واحد رایانه.

۱-۸پرسنل سازمان: هریک از افرادی که در سازمان و به هر عنوان و در هر قالبی اشتغال دائم یا موقت دارند و به هر طریق از امکانات رایانه‌ای استفاده می‌نمایند.

ماده ۲.حوزه تسری آئین‌نامه:

۲-۱.تمام سیستم‌های اطلاعاتی الکترونیکی سازمان اعم از رایانه‌ها و تجهیزات جانبی آن، نرم‌افزارها، شبکه دیتا، داده‌ها(حتی اگر از نظر فیزیکی خارج از سازمان واقع شده باشد)

۲-۲.هرگونه سیستم اطلاعاتی که کاربرد آن بر تجهیزات رایانه‌ای یا شبکه سازمان تاثیرگذار بوده اعم از آنکه متعلق به سازمان باشد یا نباشد و صرفنظر از محل استقرار آن.

۲-۳.کلیه پرسنل سازمان

فصل دوم – وظایف و مسؤولیتها

در مواد ۳ تا ۵ به بخشی از وظایف و مسؤولیت‌های مرتبط با این آیین‌نامه، توجه و تاکید شده است:

ماده ۳.وظایف و مسؤولیت‌های مشترک کلیه پرسنل سازمان

مسؤلیت‌های زیر متوجه کلیه پرسنل سازمان خواهد بود:

۳-۱.رعایت کامل این آیین‌نامه و نیز کلیه مصوبات و سیاست‌های هیئت رئیسه و مرکز رایانه، در این راستا لازم است کلیه پرسنل متناسب با مقتضیات حوزه فعالیت‌های خود تدابیر لازم را اتخاذ نماید.

۳-۲.یادگیری اصول استفاده صحیح از امکانات رایانه‌ای و حفاظت از داده‌ها و رعایت آن.

۳-۳.خودداری از کاربردهای غیر متعارفی که در مجموعه ماموریت‌ها و اهداف کاری آن‌ها نمی‌گنجد.

۳-۴.مراقبت بر حفظ شؤون سازمان و به ویژه پرهیز از تخلفات مندرج در ماده ۵ این آیین‌نامه.

ماده ٤.وظایف و مسؤولیت‌های مرجع رسیدگی و متصدیان امور رایانه

موارد زیر برعهده متصدیان امور رایانه می‌باشد:

۴-۱.برنامه‌ریزی و تلاش مناسب در راستای اجرای صحیح و کامل این آیین‌نامه

۴-۲.گزارش موارد تخلف به مقامات بالاتر، و پیگیری لازم طبق ضوابط قضایی سایبری

وظایف و مسؤولیت‌های مسئول واحد رایانه:

مسؤولیت‌های زیر متوجه مسئول واحد رایانه خواهد بود:

۴-۳.اعمال تدابیر مناسب برای اجرای کامل این آیین‌نامه

۴-۴.پی‌گیری گزارش تخلفات و اقدام مناسب در قبال متخلفان، از قبیل:

۴-۴-۱.تذکر شفاهی

۴-۴-۲.تذکر کتبی

۴-۴-۳.محرومیت از تمام یا برخی امکانات رایانه‌ای

۴-۴-۴.معرفی به مرجع رسیدگی به تخلفات رایانه‌ای به همراه ارسال سوابق مربوط

تبصره: لازم است مرجع رسیدگی به تخلفات رایانه‌ای هنگام بررسی، موارد زیر را رعایت کنند:

الف- مشورت با مرکز رایانه، جهت حضور کارشناس فنی در جلسات رسیدگی

ب- اعمال تنبیهات مؤثر بر متخلفانی که محکوم می‌شوند(تذکر، تعلیق، ...)

ج- در موارد مقتضی ارجاع پرونده به مراجع قضایی

فصل سوم – تخلفات رایانه‌ای

ماده ۵.موارد زیر، تخلف رایانه‌ای تلقی شده و ممنوع می‌باشد:

۱.دسترسی، شنود و دریافت غیرمجاز

منظور از دسترسی غیر مجاز، دسترسی عمدی و بدون مجوز، به داده ها یا سیستم‌های رایانه‌ای سازمان می‌باشد و منظور از شنود و دریافت غیر مجاز، شنود و یا دریافت عمدی و بدون مجوز داده‌های در حال انتقال سیستم‌های رایانه‌ای سازمان می‌باشد. ازقبیل:

اطلاعات سیستم‌های آموزشی، پژوهشی، اداری و مالی و ...

دسترسی غیرمجاز به صندوق پستی یا کارتابل الکترونیکی دیگران

استفاده غیر مجاز از اکانت دیگران

داده های در حال انتقال مربوط به کلمه عبور

استفاده غیرمجاز از نرم افزارهای Monitoring

۲.جعل رایانه‌ای

هرگونه تغییر یا ایجاد، محو یا متوقف کردن داده های رایانه‌ای و دارای ارزش اثباتی سازمان که بدون مجوز صورت گرفته باشد جعل رایانه‌ای محسوب خواهد شد. ازقبیل اعمال تغییر غیر مجاز در:

لیست نمرات

ارقام و اسناد مالی

مکاتبات الکترونیکی اداری

استفاده از داده‌های جعل شده

۳.تخریب و ایجاد اختلال در داده‌ها

پاک کردن، صدمه زدن، دستکاری، غیر قابل استفاده کردن و یا به هر نحو تخریب یا مختل کردن داده‌های دیگری از سیستم رایانه‌ای یا ازحامل‌های داده، به قصد اضرار به غیر از قبیل:

دستکاری و تغییر صفحات وب شخصی

تغییر داده های رایانه‌ها یا حافظه های جانبی

۴. اختلال در سیستم

انجام اعمالی به عمد (از قبیل وارد کردن، انتقال دادن، ارسال، پخش، صدمه زدن، پاک کردن، ایجاد وقفه، دستکاری یا تخریب داده‌ها با امواج الکترومغناطیسی، یا قطع ارتباط فیزیکی) که باعث غیر قابل استفاده شدن یا مختل کردن سیستم رایانه‌ای دیگران شود مثل:

قطع کابل شبکه یک رایانه

خاموش کردن غیر مجاز هاب یا سوئیچ

انتشار ویروس

۵. ممانعت از دستیابی

ممانعت عمدی و غیر مجاز از دستیابی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای سازمان با انجام اعمالی از جمله مخفی کردن داده‌ها، تغییر رمز ورود و یا رمزنگاری داده‌ها مثل:

تغییر غیر مجاز رمز ورود افراد

ایجاد رمز یا سطح دسترسی برای داده های دیگران بدون مجوز

تغییر غیر مجاز link آدرس اینترنتی

۶.کلاهبرداری

سوء استفاده از سیستم رایانه‌ای سازمان برای تصاحب یا تحصیل مال یا منفعت یا خدمات مالی یا امتیازات مالی برای خود یا دیگری (با انجام اعمالی نظیر وارد کردن، تغییر، محو، ایجاد، توقف داده‌ها یا مداخله در عملکرد سیستم و نظایر آن)ازقبیل:

سوء استفاده در سیستم ثبت ورود - خروج و سیستم حقوق – دستمزد و استفاده شخصی از سیستم رایانه ای سازمان

۷.تولید یا نشر محتویات مبتذل و غیر اخلاقی

استفاده از سیستم رایانه‌ای برای تولید یا نشر یا استفاده شخصی یا هر گونه معاملهٔ ای که دارای محتویات مبتذل و غیر اخلاقی بوده و همچنین مشاهده و تکثیر لوح های موسیقی غیر مجاز (تصویری و غیر تصویری)

تبصره ۱: محتویات غیر واقعی نیز مشمول مقررات این ماده است.

.تبصره ۲: مفاد ماده فوق شامل آن دسته از محتویاتی که برای استفاده متعارف علمی یا هر مصلحت عقلایی دیگر ارایه می گردد، نخواهد بود.

۸.انتشار اسرار خصوصی

استفاده از سیستم رایانه‌ای برای انتشار یا در دسترس قراردادن فیلم یا تصویر یا صوت یا اسرار خصوصی یا خانوادگی دیگری بدون رضایت وی.

۹.انتشار اکاذیب

استفاده از سیستم رایانه‌ای برای انتشار یا در دسترس دیگران قرار دادن اکاذیب و نیز نسبت دادن اعمالی به شخص حقیقی یا حقوقی یا مقامات رسمی برخلاف حقیقت، حتی اگر به‌صورت نقل قول باشد.

۱۰.سایر موارد

انتشار، توزیع، یا مورد معامله قرار دادن داده‌ها یا نرم‌افزارها یا هر نوع وسایل الکترونیکی که صرفاً به منظور ارتکاب تخلفات رایانه‌ای مورد استفاده قرار می گیرند.

انتشار و در دسترس قرار دادن رمز عبور، کد دستیابی یا داده‌های رایانه‌ای یا هر نوع اطلاعات مشابه به طور غیرمجاز به نحوی که به وسیله آن سیستم رایانه‌ای یا داده‌های مربوطه قابل دستیابی باشد. ازقبیل: انتشاراکانت,proxy,dial ...

آنچه که به عنوان مقررات عمومی کشور جرم رایانه‌ای خوانده شده و در اینجا ذکر نشده است.

ماده ۶.به منظور جلوگیری از ادامهٔ ارائه یا انتشار محتویات مرکز رایانه موظف است:

۶-۱.بر محتوای داده‌ها، اطلاعات یا خدماتی که ارائه می‌دهد مطابق قوانین ومقررات سازمان، نظارت نماید.

۶-۲.به محض اطلاع از وجود محتویات وخدمات ممنوعه در هر یک از سیستم های تحت تملک یا کنترل سازمان مراجع ذیصلاح را مطلع نموده و اقدامات لازم را در جهت توقف و در صورت امکان حفاظت از مدارک تخلف به عمل آورد.