دانشگاه علوم پزشکی و خدمات بهداشتی درمانی گیلان	**سیاست های استفاده از شبکه اینترنت در دانشگاه علوم پزشکی گیلان**	کمیته امن سازی دانشگاه
کد سند: 14020313-1	ویرایش : 1	خصوصی	تاریخ تدوین: 1402/3/13

این مستند با هدف تعیین روش ها و قواعد **دسترسی به اینترنت در شبکه گسترده** دانشگاه علوم پزشکی گیلان تدوین شده است.

با توجه به تمهیدات، آسیب پذیری های متعدد و امنیت پایین تبادل اطلاعات بر بستر اینترنت به دلیل امکان نفوذ، استفاده و شنود توسط افراد غیر مجاز، این مستند با رویکردهای ذیل تدوین شده است:

1) رعایت بخشنامه های ابلاغی از مراجع بالا دستی در خصوص جداسازی شبکه داخلی از شبکه اینترنت
2) مدیریت و کاهش هزینه ها با بهره برداری حداکثری از پهنای باند اینترنت تامین شده
3) تامین حداکثری امنیت تبادل اطلاعات اینترنت در شبکه دانشگاه
4) رعایت مواد 32 و 33 قانون جرایم رایانه ای در راهبری زیرساخت شبکه دانشگاه با تاکید بر لزوم ثبت هویت کلیه کاربران هنگام استفاده و دسترسی به اینترنت

نظر به لزوم استفاده از اینترنت جهت پیش برد اهداف آموزشی و پژوهشی توسط اساتید، دانشجویان و کارکنان و همچنین قرار گرفتن بسیاری از سامانه های نرم افزاری بر بستر اینترنت، استفاده از آن توسط کارکنان و دانشجویان دانشگاه علوم پزشکی امری اجتناب ناپذیر می باشد لذا ضروری است تمهیدات لازم جهت مدیریت ترافیک اینترنت و به حداقل رساندن مخاطرات امنیتی استفاده از بستر اینترنت، از طریق روش های بهره برداری ازاینترنت در حوزه های آموزشی و درمانی به شرح ذیل تعیین و ابلاغ می گردد و از تاریخ ابلاغ رسمی رعایت آن الزامی می باشد.

مدیریت ترافیک اینترنت به دو شکل در زیرساخت سازمان امکان پذیر است:

1- روش اول کنترل دسترسی کاربر به اینترنت

در روش کنترل دسترسی، سیستم‌های سازمان به صورت پیش فرض به اینترنت دسترسی ندارند و جهت کار با اینترنت لازم است کاربر یک اتصالVPN به سرور اینترنت برقرار کند. با طی کردن این فرآیند کاربر به اینترنت دسترسی خواهد داشت.

استفاده دو منظوره از سیستم کاری، مخاطراتی به همراه دارد چرا که در صورت آلوده شدن ایستگاه کاری به واسطه فعالیت در اینترنت، علی رغم قطعااینترنت توسط کاربر، آلودگی به راحتی می‌تواند در شبکه سازمان گسترش یافته و آسیب‌های خود را وارد کند.

2- روش دوم جداسازی ترافیک اینترنت از اینترانت

در این روش نیز ترافیک اینترنت و اینترانت از طریق **فیزیکی** یا **منطقی** از هم جدا می شوند. در روش فیزیکی یک شبکه جداگانه جهت اتصال بهااینترنت در نظر گرفته می شود، این روش دارای امنیت بالاتری نسبت به سایر روش ها است بنابراین استفاده از این روش منوط به استقرار دو دستگاه مجزا، یکی صرفاً برای اینترنت و دیگری منحصراً برای شبکه داخلی سازمان خواهد بود که تنظیمات مربوطه می بایست توسط کارشناسان آی تی انجام گیرد لیکن جهت انتقال فایل بین شبکه داخلی و اینترنت نیاز به فلشUSB می باشد که خود از عوامل اصلی انتقال آلودگی و نفوذ در سیستم ها خواهدبود. در جداسازی منطقی نیز اینترنت در یک محدوده قرار می‌گیرد و کاربر با استفاده از ابزارهایی در این محیط اقدام به فعالیت با اینترنت می‌کند.،جدا سازی منطقی بیشتر مناسب سیستم های کاربران داخل شبکه دانشگاه می باشد که به دلیل پیچیدگی و هزینه بالا فعلاً در دستور کار نمی باشد و درصورت تأمین اعتبار توسط واحدهای تابعه مجوز آن صادر و پروتکل مربوط به همراه مجوز ابلاغ می گردد.

رایانه ها و تجهیزاتی که از اینترنت دانشگاه استفاده می کنند به دو گروه تقسیم می شوند:

گروه اول: دستگاه های شخصی متعلق به دانشجویان، اساتید و کارکنان می باشد که امکان نصب آنتی ویروس دانشگاه و کنترل امنیتی متمرکزبرروی

آنها وجود ندارد.

با توجه به امنیت پایین دستگاه های مذکور و تهدیدات سایبری بالقوه بالای آنها، ضرورت دارد شبکه مورد استفاده جهت اتصال دستگاه ها به اینترنت کاملا ایزوله شده و از شبکه داخلی دانشگاه که سایر سیستم ها در آن قرار دارند جدا گردد. سپس از هات اسپات جهت احراز هویت و اتصال کاربران استفاده می شود.

مدیریت قرار گرفته سپس از یک پورت دستگاه مذکور یک شبکه اختصاصی با همه اکسس پوینت ها ایجاد گردد تا بهره برداری از دستگاههای شخصی در شبکه جدید(وای فای) امکانپذیر گردد.

گروه دوم: دستگاه هایی که تحت کنترل و نظارت همکاران آی تی دانشگاه بوده و از طریق محدود سازی دسترسی کاربران و سیستم عامل های کاربران در محیط domain و همچنین نصب آنتی ویروس دانشگاه بر روی آنها از نظر آلودگی های نرم افزاری دارای امنیت بیشتری می باشند. نظر به اینکه تبادل داده های درون سازمانی از طریق این دستگاه ها انجام می شود دارای اهمیت بالاتری می باشند لذا با عنایت به امنیت پایین ضرورت دارد.

حتی الامکان از اینترنت استفاده نشود و در صورت نیاز ضروری برای دسترسی به اینترنت از طریق VPN حتماً با مسئولین آی تی مراکز هماهنگ تا بصورت کنترل شده،دسترسی های مورد نیاز ایجاد گردند.(بهترین راهکار برای این گروه از دستگاه ها استفاده از جدا سازی منطقی اینترنت از اینترانت می باشد که با توجه به هزینه های بالای آن در فازهای آتی توسعه شبکه و زیرساخت دانشگاه انجام خواهد شد)

بدین منظور مقتضی است سیاست های کلی زیر جهت استفاده از اینترنت در نظر گرفته شود

- استفاده چندین کاربر از اینترنت دانشگاه با یک نام کاربری و به صورت اشتراکی ممنوع می باشد(استفاده از NAT و یا کانکشن وی پی ان بر روی روتر ها یا دستگاه های شبکه ممنوع می باشد)
- کلیه کاربران باید از طریق سرویس مرکزی احراز هویت دانشگاه (RADIUS) متصل شوند و تعریف کاربران در واحد های تابعه ممنوع می‌باشد.
- توافقنامه پیوست این روش اجرایی، برای استفاده از اینترنت به رویت و تأیید امضای کلیه استفاده کنندگان از اینترنت برسد.

با عنایت به استانداردهای اعتبار بخشی و ضرورت تسهیل استفاده از اینترنت توسط اساتید و دانشجویان مقتضی است تأمین اعتبار و پیگیری جهت آماده سازی زیرساخت لازم برای دریافت سرویس HotSpot صورت گیرد:

1- قرار گیری یک دستگاه روتریا فایروال یا سوئیچ قابل مدیریت در لبه شبکه(در صورت وجود هریک از دستگاهها نیاز به خرید مجدد نمی باشد).
2- قرار گیری یک دستگاه روتر یا فایروال یا سوئیچ قابل مدیریت در لبه شبکه(در صورت وجود هریک از دستگاهها نیاز به خرید مجدد نمی باشد).
3- اکسس پوینت های استفاده شده در نقاط مختلف شبکه باید با دستگاه قرار گرفته در لبه شبکه اتصال مستقیم داشته باشند، به این منظور باید شبکه فیزیکی جداگانه طراحی و پیاده سازی شده و یا از طریق VLAN بندی بر روی سوئیچ های مدیریتی موجود، در لایه دوم شبکه از هم جدا گردند تا از تداخل دو شبکه و بروز اختلال در عملکرد شبکه داخلی جلوگیری شود

4- در صورت پیچیدگی شبکه در آن واحد و پراکندگی نقاط اتصال می توانید از طریق برون سپاری به شرکتهای پیاده سازی شبکه جهت برآورد هزینه اولیه، کابل کشی و نصب تجهیزات مورد نیاز استفاده نمایید(اخذ مجوز فنی از این مدیریت الزامی می باشد).

5- انجام تنظیمات اکتیو و تحویل سرویس HotSpot بر روی یکی از پورتهای دستگاه لبه شبکه بر عهده کارشناسان واحد زیرساخت دانشگاه می باشد و انجام سایر اقدامات مربوط به شبکه داخلی توسط کارشناسان فناوری مراکز مربوطه انجام می گردد

پس از آماده سازی شبکه فیزیکی داخلی می بایست مراتب به اطلاع گروه زیرساخت دانشگاه رسانده شده تا تنظیمات نهایی و فعال سازی HotSpot توسط کارشناسان زیرساخت دانشگاه صورت گیرد.

مسئولیت رعایت استانداردهای فنی اعلام شده در روش اجرایی حاضر بر عهده بالاترین مقام اجرایی و مسئول فناوری آن حوزه می باشد.

توافقنامه استفاده از اینترنت

* هر دانشجو دارای حساب کاربری خاص خود جهت استفاده از اینترنت می باشد و استفاده از آن در حدود اختیارات داده شده است و تمام عملیات وی در شبکه با این شناسه ذخیره می شود و در هنگام لزوم جهت ردیابی در اختیار مراجع ذی صلاح قرار خواهد گرفت. لذا کاربران موظفند در حفظ و نگهداری کلمه عبور خود دقت کامل را داشته باشند، در صورت هر گونه سوء استفاده، مسئولیت و عواقب آن با شخص صاحب حساب کاربری است.

* شناسه کاربری نباید امانت داده شود.

* لازم است کاربران محترم آشنایی و توانایی کافی جهت کار با ویندوز و اینترنت را داشته باشند، تبعات ناشی از عدم مهارت به عهده کاربر است. (مواردی مانند آنتی ویروس هایی که دارای فایروال هستند و جلوی اتصال به اینترنت را می گیرند.)

* مسئولیت نصب نرم افزار و آنتی ویروس روی سیستم های شخصی به عهده دانشجو است . نصب نرم افزار هایی که باعث اختلال در شبکه شوند مثل Torrentو نرم افزارهای اشتراک فایل نظیر به نظیر (P2P) ممنوع است.

* تهیه و اتصال انواع دستگاههای وایرلس شخصی به دلیل ایجاد اختلال در شبکه و سرویس دهی مناسب و تضییع حقوق سایر دانشجویان ممنوع است.

* در صورت آلوده بودن سیستم به بد افزار ها (مانند آندرومدا) و نرم افزارهای غیرمجاز، علاوه بر مسدود شدن حساب کاربری، سیستم آلوده در شبکه مسدود می گردد و تا رفع مشکل آلودگی مسدود می ماند. زیرا اتصال سیستم آلوده علاوه بر اینکه باعث آلودگی شبکه می شود منجر به مسدود شدن ip های دانشگاه در اینترنت می گردد.

* تغییر کلمه عبور پس از اولین اتصال به اینترنت لازم و ضروری است.

	**سیاست های استفاده از شبکه اینترنت در دانشگاه علوم پزشکی گیلان**	کمیته امن سازی دانشگاه
کد سند: 14020313-1	ویرایش : 1	خصوصی	تاریخ تدوین: 1402/3/13

یادآوری مواد 32 و 33 قانون جرائم رایانه ای

ماده 32– ارائه دهندگان خدمات دسترسی به اینترنت موظفند داده های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره 1– داده ترافیک : هر گونه داده ای که سامانه های رایانه ای در زنجیره ارتباطات رایانه ای و مخابراتی تولید می کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می شود.

تبصره 2– اطلاعات کاربر : هر گونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورد استفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا پروتکل اینترنتی (ip)، شماره تلفن و سایر مشخصات فردی اوست.

ماده 33– ارائه دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند.