شیوه نامه درخواست و تخصیص سرور مجازی (VPS)

تهیه‌کننده: بخش هاستینگ و مجازی سازی مرکزفاوا

با همکاری بخش زیرساخت و امنیت فضای مجازی

WWW.CITC.UI.AC.IR

مرکز فناوری اطلاعات، ارتباطات و امنیت فضای مجازی دانشگاه اصفهان

مهر ۱۴۰۲

۱– هدف

هدف از تدوین این دستورالعمل، تعریف روال و الزامات موردنیاز درخواست ماشین مجازی (VPS) از واحد فناوری اطلاعات، ارتباطات و امنیت فضای مجازی است.

۲– دامنه کاربرد

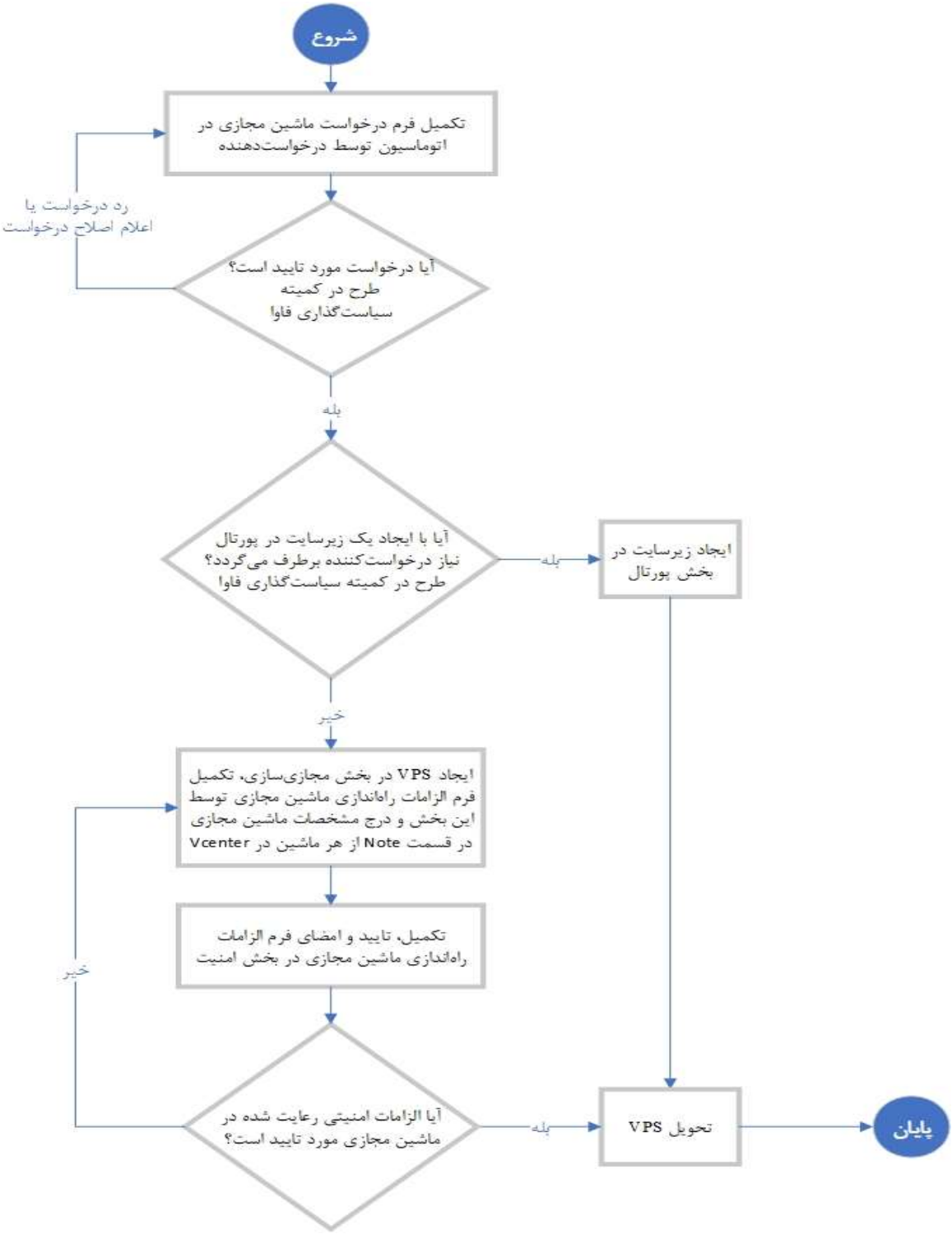
دامنه کاربرد این دستورالعمل شامل کلیه درخواست‌های واصله از اعضای دانشگاه (بهره بردار) و همچنین درخواست‌های همکاران مرکز فاوا در خصوص تخصیص ماشین مجازی جدید می‌باشد.

۳– تعاریف

- **بهره بردار:** به واحدی از بخشهای دانشگاه (معاونت، دانشکده، اداره و..) اطلاق می شود که تصمیم به راه اندازی و استفاده از سامانه ای به شکل درون سپاری یا برون سپاری شده دارد و بدین منظور سرور مجازی درخواست می دهد.
- **پیمانکار:** به شخص حقوقی اطلاق می شود که در قالب شرکت با واحد بهره بردار جهت راه اندازی سامانه مورد نظر بهره بردار، قرارداد منعقد کرده است.
- **متولی سرور:** به شخص حقیقی از پرسنل دانشگاه اطلاق می شود که از طرف واحد درخواست کننده در فرم تخصیص سرور مجازی معرفی و مشخصات دسترسی به سرور از طرف مرکز فاوا به ایشان داده می شود. این شخص به عنوان رابط بین مرکز فاوا و شرکت پیمانکار فعالیت می کند و مسئولیت تکمیل و ارسال ماهیانه فرم مربوط به چک لیستهای امنیتی سرور را به عهده دارد.

۴– شرح دستورالعمل

در این قسمت، مراحل فرآیند درخواست و تخصیص سرور مجازی (VPS) و الزامات امنیتی مورد نیاز در پیکربندی ماشین‌های مجازی پیش از تحویل آن به کاربر تشریح شده است. درخواست و تخصیص VPS در مرکز فاوا مطابق با فلوچارت زیر انجام می‌شود:


شروع
تکمیل فرم درخواست ماشین مجازی در اتوماسیون توسط درخواست‌دهنده
رد درخواست یا اعلام اصلاح درخواست
آیا درخواست مورد تایید است؟ طرح در کمیته سیاست‌گذاری فاوا
بله
آیا با ایجاد یک زیرساخت در پورتال نیاز درخواست‌کننده برطرف می‌گردد؟ طرح در کمیته سیاست‌گذاری فاوا
بله
ایجاد زیرساخت در بخش پورتال
خیر
ایجاد VPS در بخش مجازی‌سازی، تکمیل فرم الزامات راه‌اندازی ماشین مجازی توسط این بخش و درج مشخصات ماشین مجازی در قسمت Note از هر ماشین در Vcenter
تکمیل، تایید و امضای فرم الزامات راه‌اندازی ماشین مجازی در بخش امنیت
خیر
آیا الزامات امنیتی رعایت شده در ماشین مجازی مورد تایید است؟
بله
تحویل VPS
پایان

۵– امنیت سرورهای مجازی

با توجه به اینکه سرور ویندوز تحویل داده شده به بهره بردار، از طرف مرکز فاوا مجهز به آنتی ویروس معتبر و متصل به سامانه به روزرسانی وصله های امنیتی می باشد و برای سرورهای لینوکس نیز آخرین به روزرسانی سیستم عامل درخواست شده، نصب می شود و پس از تحویل سرور، مرکز فاوا نظارت و مسئولیتی در قبال فرایندهای داخل سرور ندارد ، لازم است متولی سرور توانایی لازم جهت انجام و بررسی موارد امنیتی سرور ویندوز یا لینوکس را به شرح زیر داشته باشد و در صورت مشاهده موارد مشکوک در اسرع وقت با مسئولین مرتبط در مرکز فاوا تماس حاصل نماید.

سرور ویندوز:

- به روز بودن آنتی ویروس سرورهای ویندوز و ویروس یابی دوره ای سرور
- به روز بودن سیستم عامل و اطمینان از نصب وصله های امنیتی به صورت دوره ای
- نگهداری، رعایت پیچیدگی و محافظت از رمزهای ورود و تغییر دوره ای آنها
- استفاده از ترکیب حروف کوچک و بزرگ و اعداد و علامتها با بیش از ده کاراکتر
- تغییر پورتهای ارتباطی معمول و پیش فرض پایگاه داده (SQL) از طرف پیمانکار یا بهره بردار
- پیگیری نصب و تمدید گواهی امنیتی (SSL) از طریق مرکز فاوا
- بررسی فعال بودن فایروال سرور (Windows Firewall)
- پشتیبان گیری دوره ای از داده های مهم و نگهداری آن در مکانی امن غیر از سرور اصلی

سرور لینوکس:

- به روزرسانی سیستم عامل لینوکس به صورت دوره ای
- نگهداری، رعایت پیچیدگی و محافظت از رمزهای ورود و تغییر دوره ای آنها
- استفاده از ترکیب حروف کوچک و بزرگ و اعداد و علامتها با بیش از ده کاراکتر
- تغییر پورتهای ارتباطی معمول و پیش فرض پایگاه داده (MySql) از طرف پیمانکار یا بهره بردار
- پیگیری نصب و تمدید گواهی امنیتی (SSL) از طریق مرکز فاوا
- بررسی فعال بودن فایروال سرور (iptables)
- پشتیبان گیری دوره ای از داده های مهم و نگهداری آن در مکانی امن غیر از سرور اصلی

تذکر۱: جهت بررسی موارد فوق، لازم است چک لیست پیوست، ماهیانه توسط متولی سرور تکمیل و به مرکز فاوا ارسال گردد.

تذکر۲: برای حفظ امنیت، لازم است آنتی‌ویروس‌ها و آنتی‌تروژان‌های سرور فعال و به روز باشد. همچنین رعایت موارد امنیتی و تنظیم فایروال سرور ضرورت دارد.

تذکر۳: مرکزفاوا مسئولیتی نسبت به ضعف ایمنی ناشی از نرم‌افزارها، Application ها وبرنامه‌های مورد استفاده در سرور ندارد.

تذکر۴: مرکز فاوا مسئولیتی نسبت به در اختیار گرفتن کلمه عبور سرور مجازی و سایر سرویسهای بهره بردار، توسط اشخاص ثالث ندارد.

۶– پشتیبان گیری از سرورهای مجازی

مسئولیت پشتیبان گیری از پایگاه داده و اطلاعات مهم داخل سرور بر عهده بهره بردار و متولی سرور است و مرکز فاوا مسئولیتی در قبال نگهداری به روزترین نسخه اطلاعات ندارد، این مرکز صرفاً در بازه های زمانی مشخصی از ساختار سرور مجازی رپلیکا تهیه می کند که این رپلیکا محتوی اطلاعات و داده های همان لحظه سرور و نه لزوما آخرین داده های موجود می باشد.

لازم است متولی سرور، نسخه پشتیبان از داده‌های مورد نیاز خود را در مکانی غیر سرور اصلی نگهداری نماید. در صورت بروز هرگونه مشکل و عدم توانایی بازگرداندن اطلاعات، مرکز فاوا هیچ‌گونه مسئولیتی در این زمینه ندارد.

۷– تکنولوژی های مورد استفاده :

درخواست کنندگان سرور مجازی دانشگاه موظف هستند صرفا از تکنولوژی هایی که در ذیل آمده است استفاده نمایند .

سرور ویندوز :

- زبانهای برنامه نویسی سمت سرور : آخرین نسخه به روز هر زبان برنامه نویسی تحت ویندوز
- زبانهای برنامه نویسی سمت کاربر: نامحدود
- حداقل تکنولوژی مورد استفاده NET: NET 4. به بالا

- پایگاه داده ها : آخرین نسخه به روز هر پایگاه داده
- حداقل هماهنگی و کارکرد در سرور: Microsoft IIS 7

تذکر ۱: استفاده از زبانهای برنامه نویسیOpen Source در محیط هاستینگ ویندوز طبق ضوابط باید با هماهنگی مرکز فاوا دانشگاه اصفهان اجرا شود.

سرور لینوکس :

- زبانهای برنامه نویسی سمت سرور: آخرین نسخه به روز هر زبان برنامه نویسی تحت لینوکس
- زبانهای برنامه نویسی سمت کاربر: نامحدود
- پایگاه داده ها : آخرین نسخه به روز هر پایگاه داده
- حداقل هماهنگی و کارکرد در سرور: Apache 2

تذکر ۲: درخواست کنندگان سرور مجازی موظف هستند در صورت نیاز به سرویسهای خاص و یا ماژولهای اضافی در فرم درخواست به مدیریت مرکز فاوا به صورت مشخص و واضح ، نام سرویس ها و ماژول های مورد نیاز به همراه نسخه مورد نظر خود را ارائه نمایند، مدیریت مرکز فاوا در صورت صلاحدید، به اضافه کردن آن موارد به سرویس های موجود اقدام می نماید.

تذکر ۳: به دلیل ضعفهای امنیتی وردپرس، این پایگاه داده پیشنهاد نمی شود.

در ادامه فرم‌های «درخواست ماشین مجازی» و «الزامات راه‌اندازی ماشین مجازی» که در فلوچارت به آن‌ها اشاره شده، ارائه گردیده است.

۸– تست امنیت سرورهای مجازی

جهت حفاظت بیشتر، تست امنیت سرورهای مجازی به صورت دروه ای توسط مرکز آپا دانشگاه اصفهان انجام و نتیجه تست به مرکز فاوا و واحد بهره بردار جهت انجام فعالیتهای لازم گزارش داده می شود.

شیوه نامه درخواست و تخصیص سرور مجازی

جدول ۱: فرم درخواست ماشین مجازی

فرم درخواست سرور مجازی از مرکز فاوا		
شماره فرم:		**تاریخ:**
دانشکده/واحد بهره‌بردار:	**متولی سرور: (پرسنل دانشگاه)**	**شماره تماس:**
عنوان و کاربرد سرور مجازی(VPS):		
وضعیت پشتیبانی سرور (درون سپاری یا برون سپاری):		
نام شرکت پیمانکار در صورت برون سپاری:	**مسئول مربوطه:**	**شماره تماس:**
مشخصات فنی مورد نیاز: (حداقل های لازم) CPU: RAM: HDD: نوع سیستم عامل: نوع پایگاه داده: سایر: نرم افزار مجوز افتا دارد: ☐بله ☐خیر مجوزهای دیگر:	**دسترسی‌های موردنیاز در سرور:** ☐اتصال سرور به اینترنت ☐باز شدن پورت‌های HTTP و HTTPS در داخل دانشگاه (انتشار سامانه در شبکه داخلی) ☐باز شدن پورت‌های HTTP و HTTPS از خارج دانشگاه (انتشار سامانه بر روی اینترنت) ☐دسترسی راه دور از داخل دانشگاه ☐دسترسی راه دور از خارج دانشگاه (از بستر اینترنت) سایر:	
تبصره۱: اختصاص منابع سخت افزاری به سرور مجازی بر اساس منابع آزاد موجود در مرکز فاوا صورت می پذیرد. لذادراعلام مشخصات فنی حداقل‌های لازم درنظرگرفته شود. **تبصره۲:** اتصال سرور به اینترنت به سرورهای مجازی به مدت محدود (یک هفته) و صرفا جهت نصب و به روز رسانی نرم افزارهای لازم صورت می پذیرد. **تبصره۳:** به دلیل ضعفهای امنیتی وردپرس، این پایگاه داده پیشنهاد نمی شود.		
نحوه پشتیبان‌گیری: مسئولیت پشتیبانگیری از پایگاه داده و اطلاعات مهم داخل سرور بر عهده بهره بردار و متولی سرور است و مرکز فاوا مسئولیتی در قبال نگهداری به روزترین نسخه اطلاعات ندارد، این مرکز صرفاً در بازه های زمانی مشخصی از ساختار سرور مجازی رپلیکا تهیه می کند که این رپلیکا محتوی اطلاعات و داده های همان لحظه سرور و نه لزوما آخرین داده های موجود می باشد.		
ملاحظات امنیتی: با توجه به اینکه سرور تخصیص داده شده به بهره بردار، از طرف مرکز فاوا مجهز به آنتی ویروس معتبر و متصل به سامانه به روزرسانی وصله های امنیتی می باشد و پس از ارسال مشخصات دسترسی به سرور برای متولی، مرکز فاوا نظارت و مسئولیتی در قبال فعالیتهای انجام شده بر روی سرور ندارد ، لازم است متولی سرور توانایی لازم جهت بررسی موارد امنیتی سرور نظیر به روز بودن آنتی ویروس و ویروس یابی سرور، به روز بودن سیستم عامل و اطمینان از نصب وصله های امنیتی به صورت دوره ای و نگهداری، رعایت پیچیدگی و محافظت از رمزهای ورود و تغییر دوره ای آنها را داشته باشد و در صورت مشاهده موارد مشکوک در اسرع وقت با مسئولین مرتبط درمرکز فاوا تماس حاصل نماید. به این منظور لازم است چک لیست پیوست، ماهیانه توسط متولی سرور تکمیل و به مرکز فاوا ارسال گردد.		
نصب گواهی امنیتی (SSL) و تنظیم نامه دامنه (DNS): در صورتیکه سرور مورد درخواست محتوای قابل نمایش در اینترنت (صفحه وب) دارد، لازم است پس از راه اندازی وب سرور و بارگزاری محتوا، هماهنگیهای لازم با مسئولین مرتبط در مرکز فاوا جهت نصب گواهی امنیتی و تعیین نام دامنه (بر اساس پروتکل نامگذاری دامنه) صورت پذیرد.		
تایید موارد فوق و امضاء درخواست‌کننده	**تایید و امضاء رئیس واحد/دانشکده بهره‌بردار**	
تایید و امضاء رئیس فاوا		

جدول ۲ فرم الزامات راه‌اندازی ماشین مجازی - سرور ویندوزی

فرم الزامات راه‌اندازی ماشین مجازی – سرور ویندوزی		
کد درخواست:	نام ماشین مجازی:	
الزامات مرتبط با بخش مجازی‌سازی		
انجام شده	انجام نشده	شرح
☐	☐	نام‌گذاری ماشین مجازی مطابق با استاندارد فاوا
☐	☐	نصب و فعال‌سازی نسخه به‌روز سیستم عامل حاوی آخرین وصله‌های امنیتی منتشر شده
☐	☐	پارتیشن‌بندی هارد دیسک
☐	☐	ایجاد حساب مدیریتی جدید با نام غیر پیش‌فرض و اعطای دسترسی Admin
☐	☐	پیکربندی کلمه عبور با طول (حداقل ۱۰ کاراکتر) و پیچیدگی مناسب
☐	☐	غیرفعال‌سازی حساب کاربری Administrator
☐	☐	پیکربندی الزامات طول و پیچیدگی کلمات عبور در Group Policy
☐	☐	پیکربندی Account Lockout برای مدت ۱۰ دقیقه با سه تلاش ورود ناموفق در Group Policy
☐	☐	پیکربندی Lock Screen بر روی ۵ دقیقه
☐	☐	تخصیص Static IP متناسب با ناحیه سرور IP Address: .....
☐	☐	تخصیص نام دامنه در صورت نیاز Domain Name: .....
☐	☐	نصب SSL در صورت نیاز
☐	☐	فعال‌سازی دسترسی RDP تنها برای حساب مدیریتی ایجاد شده و تغییر پورت پیش‌فرض
☐	☐	فعال‌سازی فایروال و Windows Defender و اطمینان از مسدود بودن پورت‌ها و سرویس‌های غیرمجاز
☐	☐	نصب آنتی ویروس و اطمینان از اتصال آن با سرور مرکزی
☐	☐	اتصال سرور به WSUS
☐	☐	اتصال سرور به NTP Server
☐	☐	اتصال سرور به Log Collector
☐	☐	ثبت مشخصات سرور مطابق با «فرم درخواست ماشین مجازی» در قسمت Note ماشین مجازی
نام و امضاء کارشناس مجازی‌سازی		
الزامات مرتبط با بخش امنیت		
انجام شده	انجام نشده	شرح
☐	☐	اطمینان از پیاده‌سازی صحیح کلیه الزامات فوق توسط بخش مجازی‌سازی
☐	☐	باز نمودن پورت‌ها و دسترسی‌های موردنیاز بر روی فایروال
نام و امضاء کارشناس امنیت		

جدول ۳ فرم الزامات راه‌اندازی ماشین مجازی – سرور لینوکسی

فرم الزامات راه‌اندازی ماشین مجازی – سرور لینوکسی		
کد درخواست:	نام ماشین مجازی:	
الزامات مرتبط با بخش مجازی‌سازی		
انجام شده	**انجام نشده**	**شرح**
☐	☐	نام‌گذاری ماشین مجازی مطابق با استاندارد فاوا
☐	☐	نصب و فعال‌سازی نسخه به‌روز سیستم عامل حاوی آخرین وصله‌های امنیتی منتشر شده
☐	☐	پارتیشن‌بندی هارد دیسک
☐	☐	ایجاد حساب مدیریتی جدید با نام غیر پیش‌فرض و اعطای دسترسی Sudo
☐	☐	پیکربندی کلمه عبور با طول (حداقل ۱۰ کاراکتر) و پیچیدگی مناسب
☐	☐	غیرفعال‌سازی حساب کاربری Root
☐	☐	پیکربندی الزامات طول و پیچیدگی کلمات عبور در PAM
☐	☐	پیکربندی Account Lockout برای مدت ۱۰ دقیقه با سه تلاش ورود ناموفق در PAM
☐	☐	پیکربندی Lock Screen بر روی ۵ دقیقه
☐	☐	تخصیص Static IP متناسب با ناحیه سرور IP Address: .....
☐	☐	تخصیص نام دامنه در صورت نیاز Domain Name: .....
☐	☐	نصب SSL در صورت نیاز
☐	☐	فعال‌سازی دسترسی SSH تنها برای حساب مدیریتی ایجاد شده و تغییر پورت پیش‌فرض
☐	☐	فعال‌سازی iptables و اطمینان از مسدود بودن پورت‌ها و سرویس‌های غیرمجاز
☐	☐	نصب آنتی ویروس و اطمینان از اتصال آن با سرور مرکزی
☐	☐	راه‌اندازی و پیکربندی SELinux در صورت امکان
☐	☐	اتصال سرور به NTP Server
☐	☐	اتصال سرور به Log Collector
☐	☐	ثبت مشخصات سرور مطابق با «فرم درخواست ماشین مجازی» در قسمت Note ماشین مجازی
نام و امضاء کارشناس مجازی‌سازی		
الزامات مرتبط با بخش امنیت		
انجام شده	**انجام نشده**	**شرح**
☐	☐	اطمینان از پیاده‌سازی صحیح کلیه الزامات فوق توسط بخش مجازی‌سازی
☐	☐	باز نمودن پورت‌ها و دسترسی‌های موردنیاز بر روی فایروال
نام و امضاء کارشناس امنیت		

جدول ۴ فرم الزامات نگهداری ماشین مجازی (مخصوص بهره بردار) - سرور ویندوزی یا لینوکسی

فرم الزامات نگهداری ماشین مجازی – سرور ویندوزی یا لینوکسی		
تاریخ تکمیل:	نام ماشین مجازی:	
الزامات مرتبط با متولی سرور مجازی		
انجام شده	انجام نشده	شرح
☐	☐	بررسی فعال بودن نسخه سیستم عامل ویندوز (Activate)
☐	☐	تغییر دوره ای رمز ورود شناسه فعال جهت لاگین به سیستم عامل و ثبت آن در مکانی مطمئن
☐	☐	پیکربندی کلمه عبور با طول (حداقل ۱۰کاراکتر) و پیچیدگی مناسب (حروف کوچک، بزرگ، عدد وعلامت)
☐	☐	ویروس یابی سرور ویندوز و اطمینان از فعال بودن آنتی ویروس و اتصال آن به سرور مرکزی
☐	☐	نصب وصله های امنیتی دانلود شده و اطمینان از به روز بودن سیستم عامل ویندوز
☐	☐	بررسی فعال‌بودن فایروال و Windows Defender (ویندوز و لینوکس)
☐	☐	پیگیری نصب و فعال بودن گواهی امنیتی یا SSL (در صورت نیاز)
☐	☐	بررسی محیط سیستم عامل از نظر وجود فایلهای مشکوک بر روی Desktop یا داخل درایوها
☐	☐	پشتیبان گیری از داده ها و اطلاعات مهم و نگهداری آنها در مکانی غیر از سرور اصلی
☐	☐	
نام و امضاء متولی (بهره بردار) سرور		