	موارد امنیت شبکه	تیک انجام
	فایروال	
1	فایروالی برای حفاظت از شبکه داخلی خود در برابر دسترسی های غیرمجاز دارید.	
2	پسورد دستگاه فایروال را از حالت پیش فرض به حالت قوی تغییر داده‌اید.	
3	حالت پیش فرض برای تمام دسترسی ها به صورت All Deny در آمده است.	
4	تمام رول های فایروال مستند شده و در اختیار فرد مطمئنی است.	
5	هر هشداری بلافاصله بررسی شود.	
6	تنها از پروتکل های مسیریابی امن که از احراز هویت استفاده می‌کند، استفاده کنید.	
7	رول های فایروالی که دیگر استفاده نمی‌شود را غیرفعال کنید.	
	دستگاه های شبکه	
8	تجهیزات شبکه را فقط از فروشندگان معتبر بخرید.	
9	دانلود فایروال، آپدیت، پچ و آپگرید را از منابع معتبر انجام دهید.	
10	تمام دستگاه های شبکه از WPA2 یا WiFi Protected Access II استفاده می‌کنند.	
11	برای پایداری و سهولت در مدیریت، پیکربندی استاندارد را برای هر نوع دستگاه انجام دهید.	
12	لیست تمام سخت افزارهای شبکه شامل نام دستگاه، نوع، مکان، شماره سریال و ... را نگه دارید.	
13	پورت هایی که به دستگاه خاصی اختصاص داده نشده را غیرفعال کنید.	
14	دستگاه های مهم و حساس را در سگمنت شبکه جداگانه قرار دهید.	
15	تمام سرویس های غیرضروری روی روترها و سوئیچ ها را خاموش کنید.	
16	دسترسی فیزیکی به روترها و سوئیچ ها را مدیریت کنید.	
17	سیاست در زمینه پسورد را سفت و سخت بگیرید و پسوردهای قوی انتخاب کنید.	
18	اگر از SNMP استفاده می‌کنید، از SNMPv3 استفاده کنید نه SNMPv1/2 چون امکان هک IP هست.	
	مدیریت پچ	
19	فقط از نرم افزارهای دارای لایسنس و پشتیبانی شده استفاده کنید.	
20	آپدیت های نرم افزاری و پچ های امنیتی باید در اسرع وقت نصب شوند.	
21	نرم افزارهای بدون پشتیبانی باید از دستگاه های متصل به اینترنت حذف شوند.	
22	از راهکار مدیریت پچ استفاده کنید.(شرکت هایی در این زمینه فعال هستند.)	
	حفاظت در برابر بدافزار	
23	نرم افزار ضد بدافزار باید روی همه کامپیوترها و دستگاه ها نصب شود.	
24	نرم افزار ضد بدافزار باید همیشه آپدیت باشد.	
25	نرم افزار ضد بدافزار را برای اسکن اتوماتیک فایل‌ها و صفحات وب و بلاک کردن محتوای مشکوک، پیکربندی کنید.	

26	بررسی کنید که نرم افزار ضد بدافزار اسکن های دوره ای را انجام می‌دهد.	
	مدیریت اکانت کاربری	
27	اکانت کاربری و نام کاربری یونیک تعریف کنید.	
28	سیاست پسورد قوی داشته باشید تا تمام کاربران از پسوردهای قوی استفاده کنند.	
29	احراز هویت دو مرحله ای (2FA) پیاده سازی کنید.	
30	تمام اکانت های کاربری و صاحبان آنها را مستند کرده و نگهداری کنید.	
31	اکانت ادمین فقط برای انجام کارهای ادمینی استفاده شود.	
32	اکانت های کابران به خصوص اکانت ادمین که دیگر استفاده نمی‌شوند را حذف کنید.	
33	فقط از روش های ریموت اکسس معتبر استفاده کنید تا پایداری را حفظ کنید.	
34	برای ریموت اکسس از VPN استفاده کنید تا هنگام استفاده از شبکه های عمومی از امنیت دستگاه و اتصال مطمئن باشید.	
35	برای کارمندان و مهمانان، وای فای مهمان که از شبکه داخلی جداست تعریف کنید.	
36	کارمندان را در زمینه حملات و ریسک های امنیت سایبری آموزش دهید.	
	دسترسی به ایمیل و اینترنت	
37	برای حفاظت در برابر اسپم و فیشینگ و بدافزار از فیلترهای ایمیل استفاده کنید.	
38	راهکار فیلترینگ ایمیل را استفاده کنید.	
39	مطمئن شوید نرم افزارهای ضد بدافزار تمام محتواها به خصوص مدیا استریمینگ را اسکن می‌کند.	
40	راهکار مانیتورینگ اینترنت را برای داشتن اینترنت امن پیاده سازی کنید.	
	سیاست های IT	
41	مرتبا از تمام دیتاهای مهم تان بکاپ بگیرید.	
42	تست ری استور انجانم دهید تا از صحت عملکرد آن مطمئن شوید.	
43	تنظیمات WPS را روی تمام دستگاه های وایرلس انجام دهید.	
44	گزینه UpnP - Universal Plug n Play را غیرفعال کنید.	
45	در اشتراک گذاری فایل، پیش فرض را فقط خواندنی بگذارید و فول اکسس را فقط به ادمین بدهید.	