# Security Questionnaire

|  |  |
| --- | --- |
| Manufacturer |  |
| Model |  |
| Vendor Sales Engineer |  |
| Vendor Sales Contact Info (Email/Phone) |  |
| Date Information Provided |  |

## Ports & Services

1. Which ports and services are enabled by default when the device is shipped?
2. What is the process for disabling ports and services?
3. Are there any ports or services, which cannot be disabled?
4. Can someone port scan the device?
5. What is the recommendation when port scanning the device? Are there any specific ports to avoid?

## Security Patch Management

1. How often do you release software patches?
   1. If the user has expressed an urgent need for a fix to the software, we may issue a patch for that fix on request.
2. What’s the procedure/process for implementing these patches?
   1. The patch will normally come in the form of one or more assemblies that will need to be copied to the installation folder to replace the existing assemblies.
3. How do you analyze, research/test, plan, deploy, and back out patches if necessary?
   1. We track a combination of version numbers, change logs, and code branches to determine which out-of-cycle patches were deployed to each individual client. This allows us to target the specific version of the codebase is being used by the client along with any patches that have already been delivered and continue to add patches for that version. If patches need to be backed out or revised, we can adjust based on the information in the change log or code branch we use to track it.
4. Can patches be applied without interrupting proper operation of the device? If reboots or other interruptions are required can they be delayed or scheduled to occur at a specific time in the future?
   1. The software will need to be interrupted in order to apply the patch. This is a manual process and can therefore easily be scheduled by the person performing the work.
5. If critical patches get released, how quickly can you certify this patch and get communication out to customers?
   1. We’ve not encountered a situation where such a critical patch has been required, but if we a situation does occur where we discover a major security flaw that requires a critical patch, we can get communication out the same day that the patch is released.
6. Can you patch across the network or does user have to be on the device?
   1. The patch can be applied across the network using standard Windows remoting software such as RDP or WMI.
7. How do you respond to vulnerability reports?
   1. We will review vulnerabilities to see if they can be exploited in our software. Regardless of whether we determine if a vulnerability can be exploited, we often follow recommendations to update references to third-party dependencies. If the vulnerability can be exploited, we will provide details to our clients and recommend software updates or workarounds to mitigate the vulnerability.

## Malicious Software Prevention

1. Does the device support anti-virus or malware prevention tools? If so, please describe in general terms (e.g. Signature Based A/V, Behavior Based, Application White listing, etc.)
   1. They are supported. However, some of the more heavy-handed anti-malware policies have been known to filter our upgrades and/or patches for reasons similar to the following:
      1. The scanner found Mark of the Web on an assembly once and can no longer be convinced to trust it.
      2. There are not enough users of the anti-virus software who have indicated that our application is trustworthy.
2. How will your application respond to scanning tools such as Nessus, HFNetCheck, etc and antivirus?
   1. The application will run as normal, provided that the scanner does not quarantine any of the files used by it.
3. Other than anti-virus or malware prevention what methods or practices does the vendor recommend to mitigate risk exposure?
   1. Review Windows security patches and keep the OS up to date.
4. Does the vendor provide to or notify customers of updated anti-virus and malware prevention signatures applicable to the device?
   1. No

## Account Management

1. Does the device support individualized accounts and passwords?
   1. Yes, the software supports integration with Windows security and authentication as well as “database user” accounts whose credentials are stored in the application’s database.
2. How many accounts can be created?
   1. Indefinite
3. Are the passwords user-modifiable?
   1. If using Windows security, then users can modify their passwords through the Windows OS.
   2. If using database users, an admin must change the user’s password.
4. What is the minimum number of characters in a password?
   1. For database users, 8 is the default.
5. What characters are required or allowable in creating a password?
   1. By default, for database users, at least one uppercase letter, at least one lowercase letter, and at least one number is required.
6. Are users required to change password periodically? If yes, what is the time period?
   1. For database users, password expiration defaults to 90 days.
7. What is the method for removing, disabling, or renaming accounts?
   1. User accounts with the administrator role can use the web UI or the local manager tool to manage accounts.
8. Are there any accounts which cannot be deleted? If yes, are the passwords re-settable?
   1. No, all accounts can be deleted.
9. Is there an account lockout after X amount of failed login attempts?
   1. No
10. What user account information is logged when the device is accessed?
    1. The username, success or failure, and the roles they were granted are logged to the Windows Event Log.
11. Does the device support syslog?
    1. Perhaps, by subscribing to the Windows Event Log.
12. Does the device support SNMP?
13. What logs can be accessed locally?
14. What is the maximum number of entries in the access logs?

## Security Status Monitoring

1. What capabilities does the device possess for monitoring and detecting cyber security incidents?
2. Does the device have the capability to issue alerts if incidents related to security are detected?

## Disposal or Redeployment

1. What is the policy regarding critical cyber assets returned to vendor for repair?

## Other

1. Does the device use a publicly recognized, general-purpose operating system (Windows, MS-DOS, Linux, UNIX and “UNIX-like”, Apple/Macintosh)?
2. For applications to be loaded on device:
   1. List the account/identity and privileges under which applications must run
   2. List the ability of the application to change the configuration of the device
   3. List the ability of the application to remove/install additional software
3. Is the device capable of routing IP traffic? If so, can IP routing be disabled?
4. Does the device have a wireless interface? If so, can it be disabled?
5. Does the device support DHCP? If so, what options are supported?