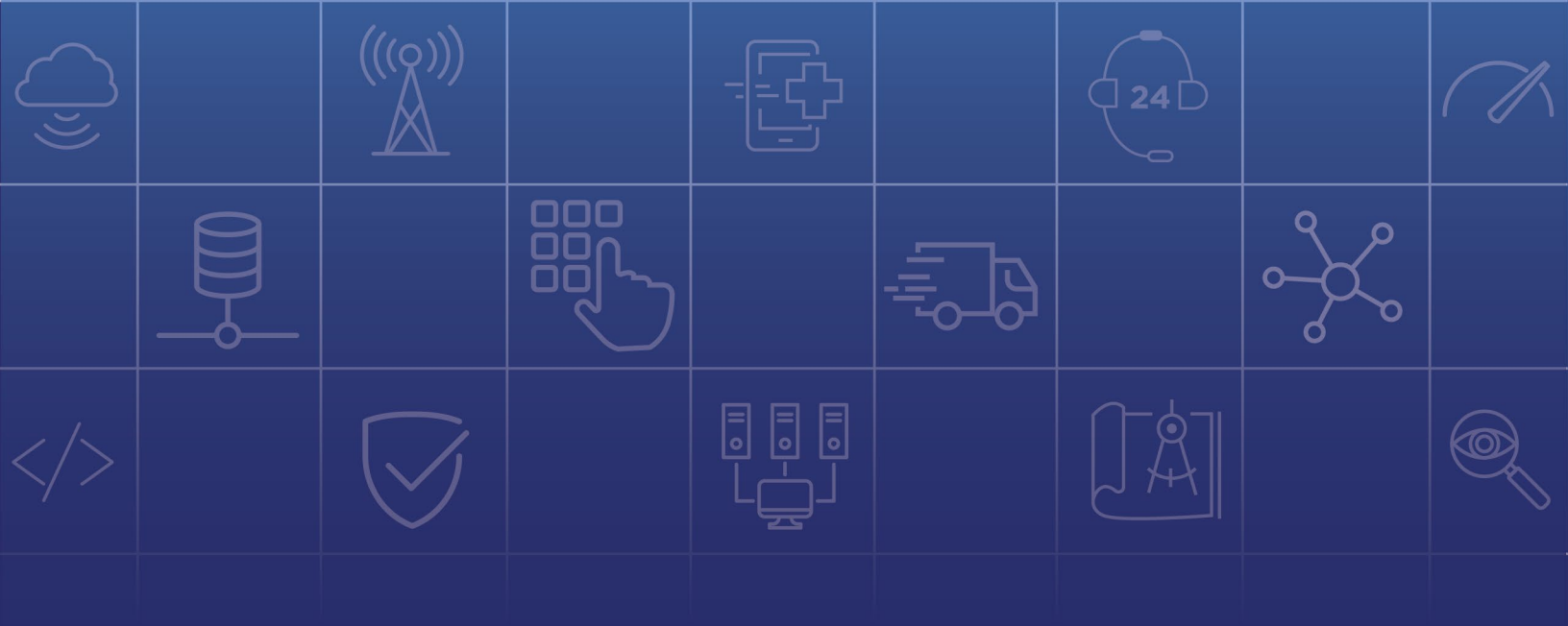

The SIGNET Advantage

Basic Security and Mission Critical Plan

(Contains specifically the below)

Annual Security Test & Inspection / Preventative Maintenance

Scope – SIGNET will test and inspect the entire Security system at each location outlined in the Statement of Work.

Testing Frequency – SIGNET will perform testing on the system on an annual basis. This includes a complete inventory of all system components complete with unique identifiers affixed or near each device.

Preventative Maintenance – Inspections will be scheduled detailing the tasks to be performed, the skill levels required, and any special tools and instrumentation required to properly maintain the systems. Upon completion of each Inspection, a summary of the tasks completed will be provided to the client.

Video Surveillance / CCTV (if applicable)

- Inspect CCTV cameras, verify and correct camera field of view and focus.
- Clear system devices of dust or debris
- Verify cameras are viewing the desired image by the client.
- Verify camera programming, naming, image quality, settings and recording settings.
- Verify system is recording and note retention period.
- Verify recording hard drive configuration and status. Check for drive failures or bad sectors.
- Verify motion detention recording settings. Verify all cameras are capturing the expected motion activity. Note any discrepancies.
- Verify PTZ control of applicable cameras. Check presets, tours, and home position settings.
- Verify all channels of the video encoder(s) are working properly.
- Verify camera call-up upon event/alarm where applicable.
- Verify network switch utilization and network switch ports are functioning.
- Check system alarm and event logs. Attach a printed copy of the logs if applicable.
- Verify system time of day is configured and is synchronizing with a time server or consistent source.
- Verify and note current software version and device firmware versions.
- Verify client and server computer hardware specifications. Verify CPU, memory, and network utilization. Note performance stats. Perform reboot of all computers and verify system back online and note any changes in performance stats.
- Provide written report to end user stating the above is working properly.

Access Control (if applicable)

- Check access control panel/controller communications status.
- Check access control panel/controller batteries. Note battery type, voltage amp-hour rating and date code. Test and note battery voltage.
- Inspect door hardware for operation, damage, and misalignment.
- Inspect and test operation of access control equipment at each door (card readers, door contacts, REX and door release push buttons where applicable).
- Test operation of ancillary access control inputs and outputs.
- Verify door programming, time schedules, access levels and door unlock schedules. Note programming operation.
- Verify photo badge reader and workstation Photo-ID call-up operation (if applicable).
- Verify access control system database is configured for a regular back-up.
- Verify network switch utilization and network switch ports are functioning.
- Check system alarm and event logs. Attach a printed copy of the logs if applicable.
- Verify system time of day is configured and is synchronizing with a time server or consistent source.
- Verify and note current software version and device firmware versions.
- Verify client and server computer hardware specifications. Verify CPU, memory, and network utilization. Note performance stats. Perform reboot of all computers and verify system back online and note any changes in performance stats.
- Provide written report to end user stating the above is working properly.

PLC System (if applicable)

- Check control panel/controller communications status.
- Check control panel/controller batteries and UPS's. Note battery/UPS type, voltage amp-hour rating and date code. Test and note battery voltage.
- Inspect door hardware for operation, damage, and misalignment.
- Inspect and test operation of control equipment at each door (door contacts and door release push buttons and intercoms where applicable).
- Test operation of ancillary control inputs and outputs.
- Verify control system database is configured for a regular back-up.
- Verify network switch utilization and network switch ports are functioning.
- Check system alarm and event logs. Attach a printed copy of the logs if applicable.
- Verify system time of day is configured and is synchronizing with a time server or consistent source.
- Verify and note current software version and device firmware versions.
- Verify client and server computer hardware specifications. Verify CPU, memory, and network utilization. Note performance stats. Perform reboot of all computers and verify system back on-line and note any changes in performance stats.
- Provide written report to end user stating the above is working properly.

Other Systems (Intrusion/Duress/Other) (if applicable)

- Check each intrusion motion detector, intrusion door contact, glass break device, duress button and keypad to verify its working properly (if applicable).
- Inspect and test other initiating devices or field based system components. Verify system receives state or alarm change
- Inspect and verify head end panel is clear of faults, receiving alarms, communicating with network and providing expected functionality
- Perform system reboot as applicable
- Clear head end panel or system devices of dust or debris
- Provide written report to end user confirming completeness and results of tests

Hardware Support – SIGNET will perform scheduled maintenance services on the equipment covered under this agreement.

Components and parts on the system that are found to be defective, have failed operationally, or which exhibit signs of near-term failure will be identified during each preventative maintenance inspection or test. If the component is covered under a current factory warranty, the said part or component will be replaced at no charge to client. If the component is not covered under a current factory warranty, a quote for a replacement part will be provided. For any equipment requiring repair or replacement, a billable labor estimate (to be performed during normal business hours) will be prepared and submitted for approval.

Work authorization shall be issued in writing to SIGNET by an authorized representative of the client before proceeding with the work.

Inspection Reports – SIGNET will furnish a written report certifying that such tests and inspections have been completed documenting any deficiencies found which may require corrective action.

Annual Software Upgrade Visit

SIGNET will provide a system software upgrade for the applicable Security Systems on an annual basis. The upgrade will consist of upgrading all system servers, workstations, and end-point firmware (as required for compatibility) to the latest software version (if applicable). Upgrade is dependent upon the Clients existing infrastructure's ability to support the updated systems specification requirements. *Upgrade does not include server/workstation OS updates. If applicable, OS security patches will be applied during upgrade as applicable/available and supported by the application.