convergint®

Reduce cost of system ownership and **ensure safest facilities** with preventive maintenance

Convergint **value**

Do security systems undergo planned preventive maintenance (PPM)? Just like any other critical building system, security systems like access control and video require consistent, proactive PPM to maximize uptime and help reduce the likelihood of **unexpected critical system failures**. Instead of leaving security systems in a **run-to-fail maintenance model**, imagine a world in which these systems operate with **minimal downtime and maximum reliability**, reducing both risk and overall cost of system ownership.

Convergint concentrates on addressing these vulnerabilities and potential risks by mitigating critical issues – all proactively, long before any incident occurs. Leveraging its preventive maintenance services, Convergint focuses on protecting valuable assets, people, and property, providing peace of mind to clients, and creating a safe, secure environment for all.

Key **features**

✅ **Regular maintenance schedule**
- Tailored plan for the specific needs
- Scheduled maintenance at agreed upon interval
- Identified potential issues before they become critical

✅ **Experienced technicians**
- Skilled and certified professionals with expertise in security system maintenance
- Dedicated team committed to ensuring the smooth operation of the security systems

✅ **Detailed reporting**
- Receive documentation detailing system health and maintenance activities
- Gain valuable insights into system perfomance and areas for improvement
- Enable informed decision-making for upgrades or enhancements

✅ **Customized solutions**
- Tailored preventive maintenance packages to suit the facility's requirements
- Flexible service options based on the budget and priorities

Setting the standard for **service**

✓ Why is preventive maintenance important?

Consider the following risks when preventive maintenance is neglected:

- **Unexpected critical system failures:** Unplanned downtime or failures jeopardize safety and tend to happen at the worst possible time.

- **Frequent system failures:** Without regular maintenance, system failures are more likely, resulting in higher service call rates and issue severity.

- **Inadequate testing:** Superficial checks and everyday usage are insufficient to ensure the system functions as intended.

- **Extended repair times:** Reactive repairs may result in longer component or system downtime

- **Rising costs:** Choosing run-to-fail over proactive maintenance increases long-term ownership costs.

- **System obsolescence:** Neglecting end-of-life or upgrade needs leads to system obsolescence and incompatibility with new technology.

- **Cost overruns:** A reactive repair approach leads to unexpected expense overruns from unplanned repairs and failures.

- **Nonconformity to design intent:** Neglecting maintenance deviates from the design intent, risking security and functionality.

✓ Checklist

Has the access control system been tested and inspected at least annually, including:

- ☑ Site and system walk including a visual inspection of all components
- ☑ Door locking hardware – are all devices securely mounted and free from damage?
- ☑ Inspect and clean devices for debris or environmental damage, or advise replacement
- ☑ Confirm valid and invalid card reads
- ☑ Test door forced and door held open for alarm
- ☑ Confirm Request to Exit (REX) releases door
- ☑ Confirm head-end terminations and network connection
- ☑ Check power supplies, surge protectors, and UPS systems to ensure stable power delivery to system components

Have the cameras and VMS been tested and inspected at least annually, including:

- ☑ Regularly clean camera lenses, housing, and other components
- ☑ Focus and adjust camera lenses, as necessary
- ☑ Monitor storage capacity and performance
- ☑ Review network infrastructure; identify network congestion, latency, or bandwidth issues.
- ☑ Address any network related problems that could impact video streaming or system communication.
- ☑ Test redundancy mechanisms to verify data can be successfully restored in case of a failure.
- ☑ Check power supplies, surge protectors, and UPS systems to ensure stable power delivery to system components.
- ☑ Review settings and configurations to prevent false alarms or missed events.