ROBOTIC SYSTEM DATASHEET

Model: CyberGuard-X200

BASIC INFORMATION

Model Number:	CyberGuard-X200
Manufacturer:	SecureBot Industries
Type:	Autonomous Security Robot
Production Year:	2024
Certification:	ISO 27001, IEC 62443
Operating System:	ROS2 Humble on Ubuntu 22.04 LTS

TECHNICAL SPECIFICATIONS

Dimension (L×W×H):	120cm × 80cm × 150cm
Weight:	85 kg
Battery Life:	12 hours continuous operation
Charging Time:	4 hours (fast charge)
Operating Temperature:	-20°C to +60°C
IP Rating:	IP65 (dust and water resistant)
Maximum Speed:	3.5 m/s
Payload Capacity:	25 kg
Sensor Range:	50 meters (360° LIDAR)
Communication:	Wi-Fi 6, 5G, Bluetooth 5.2

CYBERSECURITY FEATURES

Encryption: AES-256 for data at rest, TLS 1.3 for data in transit
Authentication: Multi-factor authentication with biometric support
Network Security: Built-in firewall, VPN support, intrusion detection
Update Mechanism: Secure OTA updates with digital signature verification
Access Control: Role-based access control (RBAC) with audit logging
Compliance: GDPR, HIPAA, SOC 2 Type II compliant
Vulnerability Management: Real-time vulnerability scanning and patching

KNOWN VULNERABILITIES & MITIGATIONS

CVE-2024-1234: Buffer overflow in sensor data processing module
Severity: High | *CVSS Score:* 8.1
Mitigation: Apply firmware update v2.1.3 or higher

CVE-2024-5678: Weak encryption in legacy communication protocol
Severity: Medium | *CVSS Score:* 6.5
Mitigation: Disable legacy protocol in settings, use modern TLS only

Physical Security: Potential tampering access through maintenance port
Severity: Low | *Risk:* Physical access required
Mitigation: Secure maintenance port with tamper-evident seals

REGULATORY COMPLIANCE

Standard	Status	Certificate ID
ISO 27001:2013	Certified	ISO27001-2024-001
IEC 62443-3-3	Certified	IEC62443-2024-007
NIST Cybersecurity Framework	Compliant	NIST-CSF-2024-012
EU GDPR	Compliant	GDPR-CERT-2024-089
FCC Part 15	Certified	FCC-ID-2024-XYZ123

SECURITY RECOMMENDATIONS

1. **Regular Updates:** Install security patches within 48 hours of release
2. **Network Segmentation:** Deploy robot in isolated network segment
3. **Monitoring:** Implement continuous security monitoring and logging
4. **Access Control:** Limit administrative access to authorized personnel only
5. **Incident Response:** Have incident response plan ready for security events
6. **Backup:** Regular backup of configuration and operational data
7. **Physical Security:** Secure robot storage and charging areas
8. **Training:** Provide cybersecurity training for all operators

For technical support or security inquiries, contact: security@securebot.com
Document Version: 1.0 | Last Updated: January 2024