www.oxmaint.com

Firewall Monitoring Terminal Inspection Checklist

No	Inspection Item	Status	Remark
1	Terminal is located in a secure, access-controlled area	OK / Faulty	
2	Physical locks and security mechanisms are functioning	OK / Faulty	
3	Video surveillance is operational and covers the terminal	OK / Faulty	
4	Environmental controls (temperature, humidity) are appropria	OK / Faulty	
5	All cables are securely connected and properly labeled	OK / Faulty	
6	All LED indicators show normal operation	OK / Faulty	
7	Power supply is functioning normally	OK / Faulty	
8	Cooling fans are operational and clean	OK / Faulty	
9	No unusual sounds or vibrations from the terminal	OK / Faulty	
10	Hardware redundancy components are functioning (if applicabl	OK / Faulty	
11	CPU utilization is within acceptable thresholds	OK / Faulty	
12	Memory usage is within acceptable limits	OK / Faulty	
13	Disk space/storage utilization is below critical threshold	OK / Faulty	
14	Network interface utilization is balanced and within limits	OK / Faulty	
15	No performance degradation during peak traffic periods	OK / Faulty	
16	Firewall firmware/software is current with latest stable ver	OK / Faulty	
17	Security patches and updates are applied within SLA timefram	OK / Faulty	
18	Monitoring software is up-to-date and functioning	OK / Faulty	
19	Signature databases (IPS/IDS) are updated automatically	OK / Faulty	
20	Update failure notifications are properly configured	OK / Faulty	
21	User access lists and permissions are up-to-date	OK / Faulty	
22	Multi-factor authentication is enabled and functioning	OK / Faulty	
23	Admin account passwords meet complexity requirements	OK / Faulty	
24	No shared accounts are in use for admin access	OK / Faulty	
25	Failed login attempt lockout policies are active	OK / Faulty	
26	Alert thresholds are appropriately configured	OK / Faulty	
27	Alert notifications are being sent to correct recipients	OK / Faulty	

28	Log collection and forwarding is functioning	OK / Faulty	
29	Dashboard displays are accurate and current	OK / Faulty	
30	Critical event escalation procedures are documented and test	OK / Faulty	
31	Firewall ruleset is properly documented and version controll	OK / Faulty	
32	No unused or overlapping rules exist in the configuration	OK / Faulty	
33	Default deny policy is in place for inbound traffic	OK / Faulty	
34	Rules are ordered efficiently for optimal performance	OK / Faulty	
35	Rule usage statistics are monitored for unused rules	OK / Faulty	
36	Configuration backups are performed automatically on schedul	OK / Faulty	
37	Backup files are stored securely with encryption	OK / Faulty	
38	Recovery procedures are documented and tested	OK / Faulty	
39	Backup success/failure notifications are functioning	OK / Faulty	
40	Offline backup copies exist in a separate location	OK / Faulty	
41	Logs are being captured for all relevant security events	OK / Faulty	
42	Log storage capacity is sufficient for retention requirement	OK / Faulty	
43	Logs are synchronized with accurate time source (NTP)	OK / Faulty	
44	Logs are being forwarded to SIEM or central repository	OK / Faulty	
45	Audit trails for administrative actions are complete	OK / Faulty	
46	Configuration complies with organizational security policies	OK / Faulty	
47	Industry-specific compliance requirements are met	OK / Faulty	
48	Documentation is updated and accessible for audit purposes	OK / Faulty	
49	Vulnerability scanning is performed on schedule	OK / Faulty	
50	Previous audit findings have been addressed and remediated	OK / Faulty	

Technician Signature: _____ Barcode: [ ]