Work-from-Home Security Checklist

To make sure you haven't forgotten any of the critical factors during this massive work-from-home transition, here is a brief checklist that you can use to ensure that your company's security is where it needs to be.

	WHAT TO DO	WHY TO DO IT
○	Verify & Strengthen Password Policies	Strong password policies reduce the chances of an attacker penetrating the company's local network by brute-forcing an employee's account
○	Minimize Access Rights to Internal Resources	Minimizing access means fewer opportunities for an insider or external attacker to steal sensitive information by penetrating the local network from an employee's home computer
○	Secure Employee Devices Connected to the Corporate Network	Secure employee workstations reduce the likelihood that an employee's device could be infected with malware and spread it to the local network
○	Train Employees on Identifying Potential Security Threats	An informed workforce is your first line of defense against social engineering attacks
○	Monitor the Network Perimeter Non-stop	It will be more difficult for an external attacker to penetrate the local network if remote access interfaces are secure and the network perimeter is monitored constantly
○	Log Security Events on Workstations & Servers on the Local Network	Improper employee actions and attacks on corporate resources cannot always be monitored—incident reaction and investigation improves when security events are logged
○	Use Gateways for Remote Connections Instead of a Specific Workstation	Gateways for remote connections reduce the chance that an employee workstation could be compromised in a targeted attack
○	Retain Copies & Perform Automated Deep Analysis of Network Traffic	Indicators of advanced attacks aren't always obvious at first—retaining this data can be key in identifying, preventing and recovering from advanced attacks
○	Keep a Security Operations Center On-Call to Monitor Protection 24/7	Responses to detected security incidents happen faster with 24/7 monitoring, reducing the ability for cyberattacks to inflict damage
○	Maintain Segmentation of Internal Networks	Segmenting internal networks helps to keep key business systems from being compromised by an external or internal attacker
○	Strictly Control Access to Key Segments & Systems	The more granular your access policy is, the more secure it is—always use the principal of least privilege
○	Maintain Extra Capacity to Handle Increased Workloads	Business processes are less likely to be disrupted if employees can safely connect to internal corporate resources
○	Have the IT Department Available for 24/7 Technical Support	Having IT teams available 24/7 helps prevent business processes from being intentionally disrupted by denial of service or account lockouts
○	Scan Email Attachments in a Sandbox	Testing potentially harmful email attachments in a controlled environment greatly reduces the risk of them causing a network breach
○	Monitor Security Events on Key Systems	Detection capabilities are only as effective as your ability to rapidly respond to them