CHECKLIST: BUSINESS CONTINUITY FOR REMOTE EMPLOYEES

While we hope and pray the Coronavirus will not affect you and your business or any of your employees or community, recent events compel us to offer the following advice should you need to implement a work from home plan. Cybersecurity is already a big enough concern. If you send employees to work from home and don't have a good game plan, you could be opening your business up to some big risks or threats making cybersecurity a much bigger concern.

Our goal with any of our clients is to help them have a solid strategy when it comes to implementing technology. This will allow our clients to have a functional system, productive employees and the risks have been considered and addressed.

If you're not one of our customers and you need some guidance, this checklist is meant to serve as "things you should consider" when sending your employees to work from home to allow for a functional system, productive employees and to mitigate security risks. These are all Yes/No questions. All questions are designed so that if the answer is Yes, then it is a positive or good thing. Depending on how your business network is setup, some of the questions may not apply to you. You should be especially concerned about employee owned devices (laptops or desktops, etc.) entering your network because they could have existing problems that may compromise your network.

We are available to discuss a plan to guide your organization, or you can use this information to do your best on your own to making working from home a reality if needed.

BUSINESS CONTINUITY FOR REMOTE EMPLOYEES CHECKLIST:

1) **Remote Access**
   a) Host-Based Firewall: A host-based firewall is active on workstations?
   b) Drive Encryption: Workstation hard drives are encrypted using BitLocker or third-party software where necessary?
   c) Domain Connectivity: Workstations are connected to the domain?
   d) Antivirus Software: Operating system is protected with up to date antivirus software?
   e) Antivirus Updates: Virus definitions are updated daily?
   f) Antivirus Active Scanning: An active scan is performed daily?
   g) Mobile Device Management: Are mobile devices managed using Mobile Device Management (MDM) tools?
   h) Mobile Device Encryption: Are mobile devices encrypted?
   i) Virtual Private Network: Employees remotely connect to company resources through a Virtual Private Network (VPN)?

2) **Home Wireless/Network Access**
   a) WPA2 Authentication Security: Private wireless connections use WPA2 with AES?
   b) Strong Passphrases: Private wireless connection keys use a strong passphrase?
   c) Change Default Passwords: Administrator passwords are changed from their defaults?

AZCOMP Technologies
www.azcomp.com/it | (480) 730-3055
2500 S. Power Rd, Suite 117, Mesa AZ 85209

CHECKLIST: BUSINESS CONTINUITY FOR REMOTE EMPLOYEES

3) Network Security

a) Remote Access: Does the organization define, control and review remote access methods?
b) Automated Monitoring & Control: Are automated mechanisms used to monitor and control remote access sessions?
c) Protection of Confidentiality / Integrity Using Encryption: Are cryptographic mechanisms used to protect the confidentiality and integrity of remote access sessions?
d) Telecommuting: Does the organization govern remote access to systems and data for remote workers?
e) Third-Party Remote Access Governance: Does the organization proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access?
f) Endpoint Security Validation: Does the organization validate software versions/patch levels and control remote devices connecting to corporate networks or storing and accessing organization information?

4) Cloud Security

a) Cloud Services: Does the organization facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices?
b) Cloud Security Architecture: Does the organization ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments?
c) Sensitive Data in Public Cloud Providers: Does the organization limit and manage the storage of sensitive data in public cloud providers?

5) Business Continuity & Disaster Recovery

a) Coordinate with Related Plans: Does the organization coordinate contingency plan development with internal and external elements responsible for related plans?
b) Coordinate with External Service Providers: Does the organization coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied?
c) Transfer to Alternate Processing / Storage Site: Does the organization redeploy personnel to other roles during a disruptive event or in the execution of a continuity plan?
d) Recovery Time / Point Objectives (RTO / RPO): Does the organization configure the alternate storage site to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)?

AZCOMP Technologies
www.azcomp.com/it | (480) 730-3055
2500 S. Power Rd, Suite 117, Mesa AZ 85209

CHECKLIST: BUSINESS CONTINUITY FOR REMOTE EMPLOYEES

e) Identify Critical Assets: Does the organization identify and document the critical systems, applications and services that support essential missions and business functions?
f) Resume All Missions & Business Functions: Does the organization plan for the resumption of all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation?
g) Continue Essential Mission & Business Functions: Does the organization plan for the continuance of essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and /or storage sites?
h) Resume Essential Missions & Business Functions: Does the organization resume essential missions and business functions within an organization-defined time period or contingency plan activation?
i) Contingency Training: Does the organization train applicable contingency personnel in their contingency roles and responsibilities?
j) Contingency Plan Root Cause Analysis (RCA) & Lessons Learned: Does the organization conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated?
k) Contingency Planning & Updates: Does the organization keep contingency plans current with business needs and technology changes?
l) Alternate Storage Site: Does the organization establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information?
m) Inability to Return to Primary Site: Does the organization plan and prepare for both natural and manmade circumstances that preclude returning to the primary processing site?
n) Telecommunications Services Availability: Does the organization reduce the likelihood of a single point of failure with primary telecommunications services?
o) Data Backups: Does the organization create recurring backups of data, software and system images to ensure the availability of the data?
p) Cryptographic Protection: Are cryptographic mechanisms used to prevent the unauthorized disclosure and modification of backup information?

6) Cryptographic Protections

a) Use of Cryptographic Controls: Does the organization facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies?
b) Transmission Confidentiality: Are cryptographic mechanisms utilized to protect the confidentiality of data being transmitted?

CHECKLIST: BUSINESS CONTINUITY FOR REMOTE EMPLOYEES

c) Transmission Integrity: Are cryptographic mechanisms utilized to protect the integrity of data being transmitted?
d) Encrypting Data at Rest: Are cryptographic mechanisms utilized on systems to prevent unauthorized disclosure of information at rest?
e) Storage Media: Are cryptographic mechanisms utilized on storage media to protect the confidentiality and integrity of the information being stored?
f) Availability: Does the organization have appropriate resiliency mechanisms to ensure the availability of data in the event of the loss of cryptographic keys?

7) Physical & Environmental Security

a) Physical & Environmental Protections: Does the organization facilitate the operation of physical and environmental protection controls?
b) Physical Access Authorizations: does the organization maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible)?
c) Lockable Physical Casings: Does the organization protect system components from unauthorized physical access (e.g., lockable physical casings)?

8) Third-Party Management

a) Supply Chain Protection: Does the organization evaluate security risks associated with the services and product supply chain?
b) Limit Potential Harm: Does the organization utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain?
c) Processes to Address Weaknesses or Deficiencies: Does the organization address identified weaknesses or deficiencies in the security of the supply chain?
d) Third-Party Services: Does the organization mitigate the risks associated with third-party access to the organization's systems and data?

About AZCOMP Technologies

Locally owned, AZCOMP Technologies has been providing IT solutions to small businesses since 2000. Our specialty is medical and dental practices, but we help a wide variety of small businesses by providing IT solutions, support, security, and strategy. Companies in Arizona benefit from our unique ability to consistently deliver phenomenal technology results, which includes dependable technology solutions, productive employees, minimized risk and strategic planning. Are you working with someone that can deliver such value?

AZCOMP Technologies
www.azcomp.com/it | (480) 730-3055
2500 S. Power Rd, Suite 117, Mesa AZ 85209