****

#3 Information and Data Privacy

Business Continuity Plan

|  |  |  |
| --- | --- | --- |
|  | **Part I: Business Information** | Answers & Comments |
| 1 | How many locations/branches does your operation have? |  |
| 2 | How many departments does your operation have? |  |
| 3 | Do you have an Emergency Evacuation Plan that accounts for all personnel and clearly sets forth procedures to protect life safety in the event of an evacuation, heart attack, Bomb threat, Etc? |  |
| 4 | Do you currently have a Disaster Management Program in place (including a Crisis Management plan, Department Recovery workbooks, Emergency Evacuation Plan, Etc.)? |  |
| 5 | If you have a Disaster Management Program in place is it documented and audited? |  |
| 6 | If you have a Disaster Management Program in place are your documents and  operation tested annually? |  |
| 7 | Do you have a program in place that allows you to track audit requirements for  your documentation annually so that you remain in a state of audit readiness? |  |
| 8 | If you had a disaster today, do you know how much that would cost you in lost  opportunity, recovery expenses, penalties and fees? |  |
|  | **Part II: Operational Information** |  |
| 9 | Do you have an established Local Crisis Management Team with predestinated  and well defined rolls and responsibilities? If so, is your team tested annually? |  |
| 10 | Do you have documented prioritized recovery strategies for critical departmental  processes in you operation? |  |
| 11 | Do you know how much revenue your operation would lose if you were shut down  do to an unplanned business outage, and do you know over time when that loss  would occur (Day 1, 3, 7. 30)? |  |
| 12 | Do you know who you would need to contact in the event of a disaster, and is that  list documented? |  |
| 13 | Do you have documented procedures for recovering lost or destroyed original  documents and forms? |  |
|  | **Part III: Technology Information** |  |
| 14 | If you lost your critical applications and data today, do you know how much that  would cost you in lost opportunity, recovery expenses, penalties and fees? |  |
| 15 | Do you currently have a system in place to recover lost data that is stored locally  in your office, and are those procedures clearly documented? |  |
| 16 | What are the applications that your operation relies on in order to perform your  business tasks? Are those applications hosted locally or by a third party provider? |  |
| 17 | Do you know how long it would take to recover your lost data? |  |
| 18 | If you lost access to all of you applications, do you know the priority in which  those applications would need to be restored according to potential revenue loss? |  |
| 19 | Do you currently have documented procedures to replicate your technology  infrastructure at an alternate work facility? |  |
| 20 | Do you have documented procedures that outline what you would do with your  phone system in the event of the loss of your work facility? |  |
| 21 | Are your applications accessible outside of the office? And if so, then how? |  |
|  | **Part IV: Vendor Information** |  |
| **22** | Do you know what kind of impact a disaster at your critical vendors would have  upon your operation? |  |
| **23** | Do you know what recovery time capabilities your critical vendors have in place? |  |
| **24** | Do you know if you critical vendors have plans in place that ensures the continuity  of their service to you? |  |
| **25** | Do you have an SLA with your critical vendors? |  |
| **26** | Do you have standardized documentation for inquiring about your critical vendor's  recovery capabilities and time frames? Do you know what questions to ask? |  |
| **27** | Do you know which vendors you will need to contact in order of importance in the  event of a disaster? |  |