US SIGNAL

A DR PLAN Checklist

If a disaster were to strike, are you confident that your company would be ready? If you answer "no" to any of the questions that follow, you may want to consult with a third-party company that specializes in BC/DR solutions.

A good place to start is US Signal. US Signal can assess your DR preparedness and work with you to enhance your current DR plan or devise a customized DR solution to help minimize data loss and downtime.

To request a consultation, call 866.2.SIGNAL or email us at: info@ussignal.com.

THE FIRST FIVE QUESTIONS APPLY IF YOU HAVE A DR PLAN	Y	N
Is your DR plan tested at least once a year?	○	○
When tested, does your DR plan perform as expected?	○	○
Is recovery and protection possible at the application level?	○	○
Is your DR plan resilient? Are you confident your company can continue operating even if a disaster strikes?	○	○
Does your team have the training necessary to fail over a site?	○	○

201 Ionia Avenue SW Grand Rapids, MI 49503 866.2.SIGNAL www.ussignal.com

THE NEXT QUESTIONS APPLY WHETHER YOU HAVE A DR PLAN IN PLACE OR ARE CONSIDERING ONE	Y	N
Have you conducted a business impact analysis to determine the operational, financial and reputational effects to your business if your IT assets were not available?	○	○
Have you conducted a risk assessment, or at least compiled a list of all the various disaster scenarios that could affect your company?	○	○
Do you have an inventory of your IT assets, such as hardware, software, data and applications (including any that may have been introduced due to “shadow IT”)? Does it include application and system dependencies?	○	○
Have you determined which of the above assets are most critical to keep your business operating even if a disaster strikes?	○	○
Are there any compliance or other requirements associated with your data or applications that may affect a DR plan?	○	○
Have you established RPOs and RTOs for your data and applications?	○	○
Do you currently back up your data and applications?	○	○
Are your backups kept off-site?	○	○
Do you replicate your data?	○	○
Do you currently have a hot, cold or warm site or use the cloud to minimize downtime and data loss?	○	○
Do you have any security and/or data protection solutions in place to mitigate ransomware, DDoS attacks and other cybercrimes?	○	○

NOTES: