Musarubra Resiliency Policy Statement (2022)
Revision 1.0

Musarubra Business Resiliency Management

Musarubra US LLC. strives to focus on operational resilience by integrating business continuity, crisis management, disaster recovery, emergency response, and risk management processes - all of which are designed to maintain a state of readiness to bounce back from business disruptions should they occur.

We proactively assess and work to mitigate potential disruptions through dynamic development of business continuity plans. The Musarubra US LLC. Business Continuity Management (BCM) program includes conducting various tests of these plans to seek to ensure each of the individual functions’ plans are effective and up to date. We conduct a Business Impact Analysis (BIA) at least once every two years, unless there is a significant change in our core business functions, processes or systems, in-order to assist with prioritization, planning and risk mitigation of our investments.

Musarubra US LLC. has developed a Business Continuity Plan (BCP) outlining how we respond to significant business disruptions across our critical infrastructure and global regions of operations. The Musarubra US LLC. Business Continuity Plan is designed to ensure: (i) that our critical operations will continue to function with little or no disruption, (ii) that our customers’ accounts will remain secure and accessible, and (iii) that our customers will be able to contact us, regardless of the scope of the situation or event.

The Musarubra US LLC. Business Continuity Plan (BCP), Crisis Management Plan (CMP), Disaster Recovery Plan (DRP), and Emergency Response (ER) are reviewed on an annual basis for adoption of new requirements. The validation of testing each of these plans occurs annually, or when there is a significant change to our processes or technology. The Business Impact Analysis (BIA) determines application recovery time objectives (RTO) and recovery point objectives (RPO). The Disaster Recovery exercise/ testing provide failover testing for applications and services that Musarubra US LLC. has identified as “business critical and business essential.” Outcomes from all failover testing can result in process, procedure updates and After-Action Records (AAR), which are then managed to successful resolution. All business continuity plans, crisis management plans, disaster recovery plans, and emergency response plans are audited by a 3rd party annually, based on the ISO/ IEC 22301 ISACA and NIST SP800-34x Standards.

It is our goal to recover and resume business operations as quickly as possible after a significant business disruption and respond to such disruption by safeguarding our workforce and property, as well as protecting Musarubra US LLC. vital business records, and continuing to provide service to our customers. We plan to accomplish this by leveraging the following business continuity strategy:
• Designing and deploying a highly resilient cloud-based and data center-based architecture, geographically dispersed and designed to provide redundant processing capacity.
• Relocating impacted businesses to designated recovery locations as needed.
• Designing our technology and systems to support quick and efficient recovery processes for critical business functions.
• Using business and technology teams that are responsible for activating and managing the recovery process.
• Executing a defined communication plan to ensure the Musarubra US LLC. workforce receives all applicable emergency notifications and instructions via a variety of sources, including in-building announcements, telephone contact list, toll-free phone numbers, and websites.
• Exercise and testing our recovery procedures on an annual basis.

Where applicable, Musarubra US LLC. shall also comply with:

1. FedRAMP (High and Moderate) NIST SP800-53x Standards
2. General Data Protection Regulation (GDPR) compliance requirements
3. Health Insurance Portability and Accountability Act (HIPAA) compliance requirements
4. ISO/ IEC 27001 and ISO/ IEC 22301 Standards
5. Payment Card Information (PCI) compliance requirements
6. Sarbanes-Oxley Act of 2002 (SOX) compliance requirements

Due to the nature and content of these plans (BC, CM, DR, and ER), they possess sensitive information and in no way shall this be shared with anyone outside of Musarubra US LLC. regardless of a signed non-disclosure agreement (NDA). This shall include but not limited to actual plan content details, the RTO/ RPO, risks, specific exercise/ test dates, exercise/ test results, recovery/ resumption times, recovery locations, and other information that may aid in the compromise of Musarubra US LLC. operations/ systems and, or customer information.

Significant business disruptions can vary in scope and complexity, such as a single office or facility, the immediate area where more than one office or facility is located, the city where Musarubra US LLC. facilities are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. Although Musarubra US LLC. has taken significant steps to develop and implement sound business continuity plans, Musarubra US LLC. cannot guarantee all systems shall always be available or recoverable immediately after a significant business disaster or disruption. While no Business Continuity Plan can eliminate all risk of business disruptions, Musarubra US LLC. continually assesses and updates the Resiliency Plan to mitigate risk reasonably and appropriately.