BUSINESS CONTINUITY & CONTINGENCY PLAN

Integrated Curated Holdings, LLC
2101 Pearl Street, Boulder, CO 80302
Main: 720-759-3535

Primary Contact: Stacie Craddock

Email: stacie@integrated-compliance.com

Effective Date: October 8, 2025

Next Review Due: On or before October 8, 2026

INTRODUCTION

Integrated Curated Holdings, LLC ("ICA") provides specialized consulting to registered investment advisers and related financial services entities, including compliance program design and testing, regulatory filings support, cybersecurity risk management consulting, incident response advisory, and creative services that support compliant communications and branding. Because client engagements and deadlines are time sensitive and data intensive, an interruption of people, facilities, systems, or vendors can impair service delivery. This plan describes how the Firm prepares for, responds to, and recovers from a Significant Business Disruption so that client work continues with minimal delay, sensitive information remains protected, and contractual and regulatory commitments are met.

SCOPE AND OBJECTIVES

This plan applies to all personnel, facilities, information systems, devices, and vendors that support our consulting services. The objectives are to safeguard people, preserve confidentiality and availability of client and Firm information, maintain essential operations, meet time bound client and regulatory commitments, restore normal operations in an orderly manner, and communicate promptly and clearly with clients, employees, and other stakeholders.

BUSINESS DESCRIPTION

The Firm is a Colorado limited liability company with team members in Boulder and Broomfield and with remote personnel as needed. Core services include compliance consulting for SEC and state registered investment advisers, including annual reviews, marketing rule support, Form ADV and Form CRS preparation, mock exam readiness, and books and records program design. Cybersecurity consulting includes program development aligned to industry frameworks, vendor risk management, incident coordination, tabletop exercises, and employee security awareness. Creative services include compliant content development, design, and digital asset management in support of regulated communications. The Firm does not hold client funds or securities, does not accept trading authority, and does not process securities transactions.

PLAN GOVERNANCE AND AUTHORITY

The Chief Executive Officer ("CEO") is responsible for approving the plan, overseeing annual testing, and directing plan maintenance. The CEO coordinates implementation and training and maintains incident documentation. During an incident, the CEO or designee may activate the plan, allocate resources, and approve emergency communications. The plan is reviewed at least annually and after any material change in services, systems, locations, or vendor dependencies.

EMERGENCY CONTACTS

Primary: Stacie Craddock, CEO

stacie@integrated-compliance.com

Office 720-759-3535

Mobile 303-808-0815

Secondary: Ashley Craddock, COO

ashley@integrated-compliance.com,

Office 720-759-3535

Mobile 303-718-3066

OFFICE LOCATIONS AND ALTERNATE WORK ARRANGEMENTS

The principal office is 2101 Pearl Street, Boulder, CO 80302. A second office is 16591 Peak Way, Broomfield, CO 80023. If either office is unavailable, operations shift to remote work or to an alternate site with secure network connectivity. The Firm maintains secure remote access, multi factor authentication, device management, and collaboration tools so that employees can continue client work from home or another safe location. Mail is redirected or held as appropriate, and client meetings continue via secure video or telephone.

SIGNIFICANT BUSINESS DISRUPTIONS

The Firm plans for internal disruptions such as cyber incidents, system failures, local power or connectivity loss, building inaccessibility, and key personnel unavailability. The Firm also plans for external disruptions such as severe weather, regional utility outages, public health emergencies, civic disruptions, or vendor outages. Response actions depend on severity and expected duration. They include relocating staff, activating remote work protocols, shifting workloads among team members, invoking vendor contingencies, and prioritizing deliverables tied to regulatory deadlines.

INFORMATION SECURITY AND CYBER MEASURES DURING DISRUPTIONS

Cyber risks can increase when work locations change or when attackers exploit crisis conditions. During any disruption the Firm enforces multi factor authentication for all systems, uses approved VPN or secure access gateways, restricts access by role,

increases monitoring and logging, and accelerates patching on Firm managed devices. Suspicious activity is escalated to the CEO and COO immediately. If a cyber incident is suspected, affected systems are isolated, forensics and containment begin, and the incident response checklist is followed. If personal information or nonpublic information may have been exposed, the Firm coordinates with counsel on notification obligations, assists clients in meeting their own regulatory duties, and documents the investigation and remediation.

EQUIPMENT INVENTORY AND DEPLOYMENT

The Firm maintains an inventory of Firm issued laptops, phones, and peripherals. Replacement equipment is pre configured with encryption, device management, endpoint protection, and access controls. Any approved use of personally owned devices requires enrollment in device management and adherence to Firm security standards. Asset records are updated upon issuance or return.

DATA BACKUP AND RECOVERY

Client work product, Firm records, and digital assets are stored in cloud collaboration platforms with versioning, retention, and geographically redundant backups. Backups occur automatically on a daily cadence at minimum. Recovery procedures are documented and tested. If primary systems are unavailable, the Firm restores from the most recent known good backup and continues operations using alternate devices or locations as needed. All recoveries are logged and reviewed.

FINANCIAL AND OPERATIONAL ASSESSMENTS

Although the Firm does not custody client assets, a disruption can affect staffing, facilities, vendors, and cash flow. Senior management evaluates expected duration and operational impact, prioritizes client deliverables and regulatory deadlines, and reallocates resources to maintain service levels. If a prolonged disruption threatens operations, the Firm considers additional financing or cost controls and communicates with clients regarding any impact on timelines.

MISSION CRITICAL FUNCTIONS AND SYSTEMS

Mission critical functions are those necessary to deliver consulting services, meet client and regulatory deadlines, and protect information. They include secure communication and scheduling, document and project management, data storage and backup, secure file transfer, email and messaging, endpoint management and security, and creative production software and asset libraries. The Firm maintains vendor contracts that include business continuity and information security representations. Vendor performance and incident communications are reviewed at least annually. A summary register of mission critical systems and vendor contacts is maintained in Exhibit A.

COMMUNICATIONS

If normal channels are impaired, the Firm communicates with clients and employees using alternate approved methods such as backup messaging, mobile phones, or the Firm website. Messages are clear, factual, and limited to necessary details about availability, expected restoration timelines, and any required client actions. Client confidentiality is preserved at all times. Internal call trees and distribution lists are kept current. If an extended remote period is required, updated contact information is circulated to the team to maintain service.

CRITICAL VENDORS AND COUNTERPARTIES

The Firm relies on cloud service providers, communications and productivity platforms, security and device management tools, and creative software providers. During a disruption the Firm contacts affected vendors, validates their status, and follows their recommended contingency steps. If a vendor cannot meet service levels, the Firm activates alternate tools or manual procedures to sustain essential operations until normal service resumes.

REGULATORY AND CONTRACTUAL CONSIDERATIONS

The Firm does not file regulatory forms on its own behalf similar to a registered adviser, but it supports advisory clients who face fixed regulatory deadlines such as annual ADV amendments, marketing rule documentation, and books and records obligations. During a disruption the Firm prioritizes work tied to those deadlines and communicates promptly with clients about any impact on deliverables. If a breach implicates client data, the Firm coordinates with counsel on applicable privacy notification requirements and cooperates with client led notifications or regulator inquiries consistent with contractual terms.

EMPLOYEE RESPONSIBILITIES, TRAINING, AND AWARENESS

All employees must know how to reach managers and follow safety and evacuation procedures. Employees are required to keep contact details current, complete annual BCP and security training, participate in tabletop exercises, and immediately report incidents or suspected compromise. Employees working remotely must use only Firm approved systems and storage, protect devices from unauthorized access, and follow clean desk and clear screen practices.

WORKPLACE RE ENTRY

Before returning to any affected office, the Firm verifies building safety with property management or authorities, checks environmental and health conditions, confirms that information systems are secure, and validates that mission critical functions are operating. A phased return may be used. Any temporary controls added during the disruption remain in place until management authorizes normal operations.

SUCCESSION CONSIDERATIONS

If the CEO is unavailable, the COO assumes interim management. Directors will meet within two business days to confirm interim authority and to identify a long-term successor if required. Client communication continues without interruption, and access to systems and records is maintained through role-based controls.

TESTING, MAINTENANCE, AND RECORDKEEPING

The Firm tests key elements of this plan at least annually, including contact trees, remote work readiness, restoration of files from backup, and incident response procedures. Results are documented and used to improve controls. Plan copies, prior versions, and test results are maintained and are available to employees and to regulators upon request. Current versions are posted in the designated internal location and provided in hard copy during onboarding.

ACTIVATION DURING AND OUTSIDE BUSINESS HOURS

During business hours the CEO or designee announces activation, ensures personnel safety, and initiates relocation or remote protocols. Outside business hours employees check in with their manager by phone, text, or email and then follow instructions for remote work activation. Initial messages should include the employee name, contact number, current location, and whether they can access email and Firm systems.

CLIENT NOTIFICATION

If a disruption materially affects service availability or timing, the Firm notifies impacted clients promptly, explains expected duration, provides alternatives where possible, and documents all communications. If a security incident may affect client information, communications follow the incident response plan and legal counsel guidance.

MANAGEMENT APPROVAL

The Chief Executive Officer, Stacie Craddock, has reviewed and approved this plan as reasonably designed to allow the Firm to meet obligations to clients during a Significant Business Disruption.

Exhibit A – Mission Critical Systems and Vendors

Purpose	Vendor	Account Owner	URL
File Storage	SharePoint	ICA	Sharepoint.com
Compliance	Greenboard	Firm Assigned	Greenboard.com
Email & System	Microsoft	ICA	Microsoft.com
Website	Wix	ICA	Wix.com
Website	Go Daddy	ICA	Godaddy.com
Phone System	Ring Central	ICA	Ringcentral.com

Exhibit B – Call Tree

Name	Role	Primary Caller
Stacie Craddock	CEO	
Ashley Craddock	COO	Stacie Craddock
Adam Ostermiller	CBDO	Ashley Craddock
Tammi Ellis	HR	Adam Ostermiller
Lindsay Rider	Compliance	Stacie Craddock
Kristyn Koller	Cyber	Adam Ostermiller
Deandra Miklos	Creative	Adam Ostermiller
Catherine Teichert	Compliance	Stacie Craddock
Izzy Deboub	Compliance / Creative	Lindsay Rider
Anniston Craddock	Creative	Stacie Craddock
Jordyn Bashore	Compliance / Creative	Stacie Craddock
Luke Ostermiller	Creative	Adam Ostermiller
Jennifer Stevens	Creative	Lindsay Rider