Kulture Reimagined Consulting
Incident Response Plan

1. Purpose

This Incident Response Plan (IRP) provides a structured approach to handling security incidents that may impact **Kulture Reimagined's** digital assets, intellectual property, and client data.

The goal is to **identify, contain, and mitigate risks efficiently** to minimize disruptions.

---

2. Inventory of Business Assets

Digital Assets:

- Company Website
- Google Workspace (Gmail, Google Drive)
- Zoom Account
- Acuity Scheduling Account
- Stripe Payment Account

Hardware & Network:

- Laptop
- Cellular Phone
- Router with Firewall

Intellectual Property & Data:

- Trainings, Fliers, Documents
- Client Information (stored in Google Drive & CRM tools)

3. Incident Types & Response Steps

Incident Type	Indicators	Response Steps
Phishing Attack (e.g., fake email requesting credentials)	Unexpected emails from Stripe, Google, Zoom, or Acuity	**1.** Do NOT click any links. **2.** Report the phishing attempt to the service provider. **3.** Change passwords if any login details were compromised.
Account Breach (Unauthorized Login Attempt)	Notification from Google, Stripe, or Zoom about suspicious access	**1.** Log into the affected account and review recent activity. **2.**Change passwords immediately. **3.** Enable Multi-Factor Authentication (MFA), if not already enabled.
Data Breach (Client Information Compromised)	Unauthorized access to client details in Google Drive or Acuity	**1.** Identify the extent of the breach. **2.** Restrict further access and change login credentials. **3.** Notify affected clients if necessary.
Ransomware Attack(Data locked or encrypted)	Files become inaccessible, demands for payment appear	**1.** Disconnect the affected device from Wi-Fi. **2.** Restore files from a secure backup. **3.** Run antivirus scans and update security software.
Website Hack	Unexpected content, defacement, or security warnings	**1.** Contact website hosting provider (MailChimp). **2.** Reset admin credentials and update plugins/themes. **3.** Run malware scans and restore from a clean backup.

---

4. Incident Response Process (5 Steps)

Step 1: Identify

- Monitor email alerts, login notifications, and account security messages.
- Regularly check Google Workspace security settings and Stripe account logs.

Step 2: Contain

- If an incident occurs, disconnect affected devices from the internet.
- Lock down compromised accounts by resetting passwords and enabling MFA.

Step 3: Eradicate

- Remove malware by running a full antivirus scan.
- Secure affected accounts by changing all credentials.

Step 4: Recover

- Restore backups of business-critical files (Google Drive, website data).
- Contact service providers (Google, Zoom, Stripe, MailChimp) for additional security measures.

Step 5: Review & Improve

- Document what happened and what steps were taken.
- Adjust security settings to prevent future incidents.
- Train yourself on cyber hygiene best practices.

---

5. Security Best Practices for Prevention

- Enable Multi-Factor Authentication (MFA) on all accounts (Google, Stripe, Acuity, Zoom).
- Use a Password Manager to store strong, unique passwords.
- Regularly Backup Important Files to an external drive or secure cloud storage.
- Monitor Account Activity for unusual logins or transactions.
- Run Security Updates on your laptop, phone, router, and software monthly.

---

6. Contact Information for Incident Reporting

If an incident occurs, report it immediately to the service providers:

- Google Workspace Security Center**:** https://support.google.com/accounts/answer/46526
- Stripe Security Team**:** https://stripe.com/docs/security/incident-reporting
- Zoom Security Support**:** https://zoom.us/security

Next Steps:

- **Upload this IRP to Google Drive & Print a Copy.**
- **Store emergency recovery login codes securely.**
- **Run a security check-up for Google, Stripe, and Acuity accounts today.**