# Website Update Procedure for Ryxen & The Rainmaker

## 1.0 Policy Objective & Scope

The objective of this policy is to establish a standardized, secure, and auditable process for requesting, approving, and deploying updates to the corporate websites of Ryxen and The Rainmaker. This ensures all changes are reviewed for accuracy, brand consistency, and compliance with Canadian privacy laws (PIPEDA) before going live.

This policy applies to all employees, contractors, and third-party vendors who are authorized to request or implement changes to any public-facing website owned by Ryxen or The Rainmaker, including but not limited to content updates, design changes, plugin installations, and code deployments.

## 2.0 Roles & Responsibilities

- Content Requester (e.g., Marketing Coordinator, Department Head): Initiates the update request via the SwitchDesk portal, providing clear details and rationale.
- Content Approver (e.g., Brand Manager, Director of Communications): Reviews the request for brand alignment, messaging accuracy, and legal compliance. Approves or denies within 48 hours.
- **Web Developer / IT Administrator:** Executes the approved update on the staging environment, performs quality assurance, and deploys to production. Maintains version control and backups.
- **IT Director:** Oversees the entire process, conducts quarterly audits of update logs, and ensures adherence to security protocols.

## 3.0 Core Rules & Guidelines

- All website updates must be logged in the SwitchDesk admin portal before any work begins. No direct changes to the live production environment are permitted without prior approval.
- Any update that involves collecting, storing, or displaying personal information (e.g., contact forms, newsletter sign-ups) must be reviewed by the Privacy Officer to ensure PIPEDA compliance.
- All code changes must be deployed to a staging environment first, tested for functionality and security, and then promoted to production only after successful testing.
- A full backup of the website (files and database) must be taken before any deployment to production.
- Emergency updates (e.g., security patches, critical bug fixes) bypass the standard approval workflow but must be documented and retroactively approved within 24 hours.

## 4.0 Step-by-Step Procedure / Workflow

1. The Content Requester logs into the SwitchDesk portal and navigates to the 'Website Update Request' form.
2. The Requester fills out the form with the following details: brand (Ryxen or The Rainmaker), page URL, type of update (content, design, code), description of change, and any supporting assets (images, text, links).

3. The Requester submits the form. An automated notification is sent to the Content Approver and the Web Developer.

4. The Content Approver reviews the request within 48 hours. If approved, the status is changed to 'Approved' in SwitchDesk. If denied, the Requester receives a reason and can resubmit after revisions.

5. The Web Developer receives the approved request and creates a new branch in the version control system (e.g., Git) for the change.

6. The Web Developer implements the update on the staging environment, ensuring all code follows the company's coding standards and security best practices.

7. The Web Developer performs a quality assurance check on staging, verifying functionality, responsiveness, and that no personal data is exposed unintentionally.

8. The Web Developer takes a full backup of the production website (files and database) and stores it in the encrypted cloud backup folder.

9. The Web Developer deploys the update to the production environment using the approved deployment script.

10. The Web Developer performs a post-deployment verification on the live site to confirm the update is working correctly and no errors are present.

11. The Web Developer updates the SwitchDesk ticket status to 'Completed' and adds a brief deployment note (e.g., version number, any issues encountered).

12. The Content Requester receives a notification of completion and is asked to confirm the update meets expectations within 24 hours. If not, a new request can be opened.

## 5.0 Documentation & Compliance

1. All website update requests, approvals, and deployment notes are automatically logged in the SwitchDesk admin portal with timestamps and user IDs.

2. A monthly report of all website changes is generated by the IT Director and reviewed for any unauthorized or anomalous activity.

3. Full backups of the production website are retained for a minimum of 30 days in encrypted cloud storage, with weekly backups archived for one year.

4. An annual audit of the website update procedure is conducted by the IT Director and Privacy Officer to ensure ongoing compliance with PIPEDA and internal security policies.

5. All version control repositories are stored in a private, access-controlled Git server, with commit logs retained indefinitely for audit purposes.