# B-CC IWLA Website & Digital Systems Governance Policy

*Policy for IT Committee oversight, website change control, and digital systems governance*

**Policy intent:** This policy is intended to create a clear, fair process for website and digital-system changes. It is not intended to prevent committees from promoting programs, fundraising, events, or member services. It ensures that all changes affecting the website, member portal, public-facing pages, payments, data, or third-party tools are reviewed and implemented safely.

## 1. Purpose

The B-CC IWLA website and related digital systems are shared chapter assets. They support public communications, member services, renewals, payments, events, committee information, forms, documents, and other chapter operations.

Because website changes can affect security, member experience, payment processing, chapter reputation, privacy obligations, legal/compliance considerations, and technical stability, all proposed changes that impact the website or connected digital tools must be reviewed through the IT Committee before implementation.

This policy establishes the IT Committee's responsibilities and the process other committees or members must follow when requesting website or digital system changes.

## 2. Scope

This policy applies to all chapter websites, webpages, forms, buttons, menus, links, payment tools, member portals, digital documents, email integrations, third-party services, plugins, embedded tools, analytics tools, and any system connected to or promoted through the chapter website.

This policy applies to both the public-facing website and the member-facing digital experience, including the member portal, account pages, renewal workflows, forms, payment flows, event pages, committee pages, document libraries, and any future website features or digital services.

This policy applies regardless of which committee or member originates the request.

This includes, but is not limited to:

- Adding, removing, or changing website pages, buttons, menus, forms, links, documents, images, calendars, or banners.
- Adding links to outside vendors, payment processors, registration systems, fundraising platforms, ticketing systems, merchandise platforms, sponsorship tools, or any service that receives money on behalf of, or in connection with, the chapter.
- Creating or changing online payment, renewal, event registration, sponsorship, merchandise, fundraising, reimbursement, fee-collection, or other money-receiving workflows.
- Adding plugins, scripts, tracking pixels, embedded widgets, forms, or third-party integrations.
- Changing member-facing account areas, renewal flows, checkout flows, volunteer-hour systems, directories, dashboards, or access-controlled features.
- Publishing committee-specific content that changes how members or the public interact with the chapter online.
- Adding, changing, or removing website features, public-facing pages, or member portal capabilities.

## 3. IT Committee Responsibilities

The IT Committee is responsible for governance, review, implementation oversight, and technical stewardship of the chapter's website and connected digital systems.

1. **Website administration and technical maintenance.** The IT Committee manages or oversees the technical configuration, structure, access controls, plugins, themes, templates, forms, integrations, hosting-related considerations, and website administration practices used by the chapter.
2. **Website feature governance.** The IT Committee is responsible for reviewing and approving what features the website offers, including new functionality, changes to existing functionality, and removal of outdated or risky features.
3. **Member portal governance.** The IT Committee is responsible for the structure, functionality, security, access controls, and user experience of the member portal and related member-facing pages.
4. **Public-facing page governance.** The IT Committee is responsible for ensuring public-facing pages, menus, calls to action, forms, links, and workflows are technically sound, consistent with the site structure, and appropriate for publication.
5. **Security and privacy review.** The IT Committee reviews proposed changes for security risks, privacy concerns, data handling, member information exposure, account access, payment risk, vendor reliability, and overall website integrity.
6. **Vendor and integration review.** Any third-party tool that collects money, personal information, member data, form responses, registrations, analytics, or other operational information must be reviewed by the IT Committee before being linked from, embedded into, or promoted through the chapter website.
7. **Payment and money-receiving workflow review.** Any tool involving payments, collection of money, financial transactions, refunds, fees, invoices, processing charges, sponsorship funds, event fees, or financial records must be reviewed by the IT Committee in coordination with the Treasurer and the requesting committee.
8. **Website user experience and consistency.** The IT Committee ensures proposed changes are consistent with the site's design, navigation, accessibility, mobile usability, content structure, and existing member workflows.
9. **Change control and implementation.** The IT Committee determines the safest and most appropriate way to implement approved changes, including whether changes should be made by an IT Committee member, a designated website administrator, or an approved vendor.
10. **Documentation and audit trail.** The IT Committee maintains a record of approved website changes, major integrations, vendor links, access permissions, contracts, vendor payments and technical decisions.
11. **Emergency support.** The IT Committee may make emergency changes when needed to protect the website, prevent fraud, correct broken functionality, remove inaccurate or harmful content, or respond to security issues.

## 4. Committee Responsibilities

Other committees and members are responsible for identifying their communication, fundraising, program, event, operational, or member-service needs and submitting website-related requests to the IT Committee before taking action.

Committees and members may propose website content, functionality, tools, or workflows, but they may not independently publish, embed, install, authorize, or direct changes that affect the website, member portal, public-facing pages, payment workflows, or any connected digital system unless the IT Committee has reviewed and approved the change.

Committees are responsible for providing:

- The purpose of the requested change.
- The exact wording, images, links, documents, or form fields requested.
- The desired location on the website or member portal.
- Any deadlines, event dates, or launch timing.
- The name of any proposed vendor or external platform.
- Whether the request involves payments, receiving money, member information, personal data, event registration, email lists, or restricted member access.
- The committee contact responsible for answering follow-up questions.

## 5. Website Change Request Process

All website-impacting requests must follow this process.

### Step 1: Submit the request

The requesting committee or member submits a website change request to the IT Committee using the approved request method, such as email, form, or ticket system. The request should include enough information for IT to understand the purpose, content, timing, and potential impact.

### Step 2: Initial IT review

The IT Committee reviews the request for technical feasibility, security and privacy impact, member data impact, payment or money-receiving implications, website design and navigation impact, compatibility with existing systems, risk of broken links or duplicate workflows, and need for Board, Treasurer, Membership, Communications, or other committee approval.

### Step 3: Cross-functional review, if needed

Some requests require review by more than one group. For example, a payment vendor may require IT Committee, Treasurer, requesting committee, and Board review. A membership or renewal workflow may require IT Committee, Membership Committee, and Treasurer review.

### Step 4: Approval decision

The IT Committee may approve, approve with modifications, defer, or reject the request. Approval may be conditional on use of a different vendor, additional security or privacy review, revised wording, Treasurer approval, Board approval, testing before publication, or use of a chapter-controlled process instead of a third-party process.

### Step 5: Implementation

Approved changes will be implemented only by the IT Committee, an authorized website administrator, or an approved technical vendor. Requesting committees should not directly edit, install, embed, or publish website-impacting changes unless explicitly authorized by the IT Committee.

### Step 6: Testing and confirmation

Before or immediately after publication, the IT Committee will verify that the change works as intended, does not break existing functionality, and does not create unacceptable security, payment, privacy, or usability issues. For higher-risk changes, the IT Committee may require testing in a non-public environment before the change goes live.

### Step 7: Documentation

The IT Committee will document the approved change, including the requestor, approval date, implementation date, vendor or tool used, affected pages, and any follow-up obligations.

## 6. Third-Party Vendor, Payment, and Money-Receiving Requirements

No committee may independently select, publish, embed, or link to a third-party vendor, payment processor, fundraising platform, event-payment tool, sponsorship payment tool, merchandise/payment tool, financial collection platform, embedded form, or external money-receiving workflow on the chapter website without IT Committee review.

Before any such vendor or tool is linked, embedded, or promoted through the website, the requesting committee must provide:

- Vendor name and website.
- Purpose of the vendor or tool.
- Fees, processing costs, refund costs, and any hidden charges.
- Who controls the account.
- Who receives funds and where funds are deposited.
- Refund process and dispute process.
- Data collected from members, visitors, participants, sponsors, payers, or other users.
- Vendor privacy policy and terms of service.
- Whether the vendor supports reporting needed by the Treasurer.
- Whether funds flow directly to a chapter-controlled account.
- Whether multiple authorized administrators can be assigned with appropriate controls.
- Whether the tool creates any duplicate or conflicting process with existing chapter payment, membership, renewal, or reporting systems.

The IT Committee may require that payment or money-receiving tools be configured so that:

- Funds go only to official chapter-controlled accounts.
- At least two authorized chapter officers or administrators have access.
- No individual committee member has sole control over funds, reports, or payment configuration.
- Financial records are exportable for Treasurer review.
- The vendor or tool does not create confusing or competing payment workflows.
- The website clearly identifies that the payment flow, vendor, or external page is official and approved.
- The tool is removed or disabled if it becomes risky, unsupported, inaccurate, or inconsistent with chapter governance.

*This is not meant to slow down chapter initiatives. It is meant to protect the chapter, members, payers, volunteers, and committee leaders from avoidable financial, reputational, privacy, or technical risk.*

## 7. Access Control

Website administrative access will be granted only by the IT Committee or another authorized website administrator under IT Committee oversight.

Access will follow the principle of least privilege, meaning users receive only the level of access needed for their role.

The IT Committee may remove or reduce access if a user no longer needs access, changes role, creates a security risk, makes website changes outside the approved process, shares credentials, or otherwise compromises website governance.

## 8. Emergency Changes

The IT Committee may make emergency changes without prior committee approval when necessary to remove malicious, fraudulent, inaccurate, or harmful content; disable a broken or risky link; protect member data; stop a security incident; prevent payment or money-receiving errors; restore website functionality; or correct a public-facing issue that could damage the chapter's reputation.

Emergency changes should be documented and reported to the relevant committee or officers as soon as practical.

## 9. Examples of Changes Requiring IT Committee Review

The following require IT Committee review before implementation:

- Adding any button, link, page, form, or workflow that collects money or directs users to a money-receiving process.
- Linking to a new fundraising, payment, sponsorship, merchandise, ticketing, event-payment, or registration platform.
- Adding an event registration form.
- Embedding a payment page or third-party form.
- Adding a new plugin, script, integration, tracking pixel, analytics tool, or embedded widget.
- Creating a new member form or changing an existing form.
- Changing renewal, checkout, invoice, payment, or account language.
- Updating the member portal, member account area, member dashboards, or access-controlled pages.
- Changing menus, navigation, public-facing calls to action, or homepage buttons.
- Adding committee pages or changing the structure of public-facing pages.
- Adding document libraries or file-download systems.
- Adding public-facing sponsor, vendor, partner, or external platform links.
- Changing website banners, homepage content, or major visual elements.
- Creating QR-code workflows that send people to website forms or payment pages.
- Publishing any tool that collects member, visitor, payer, sponsor, donor, registrant, or payment information.
- Adding, removing, or materially changing any website feature.

## 10. Examples of Routine Content Requests

Some lower-risk content requests may be handled through a simpler review, as long as they do not involve payments, receiving money, vendors, personal data, forms, login areas, scripts, plugins, or major navigation changes.

Examples may include:

- Updating committee meeting dates.

- Posting approved event descriptions.
- Replacing a page image.
- Updating officer or committee contact information.
- Uploading approved documents.
- Updating text on an existing page.

The IT Committee may create a faster process for routine content updates.

## 11. Decision Authority

The IT Committee has authority over technical implementation, website features, member portal functionality, public-facing page structure, website security, access control, vendor integration, and whether a proposed change is technically appropriate for the website.

The IT Committee does not replace the authority of the Board, Treasurer, or other committees over their subject matter. Instead, the IT Committee ensures that approved chapter activities are implemented safely, consistently, and responsibly on the website.

Where a request involves both technical and financial or policy decisions, approval must include the Board of Governors and any other appropriate responsible parties.

## 11A. Major Change Governance and High-Risk Action Approvals

Certain high-impact website or digital-system changes require elevated governance due to their potential financial, legal, operational, or reputational consequences. These “Major Changes” may not be implemented, initiated, or approved solely by the IT Committee.

Major Changes require approval from the IT Committee Chair AND Board of Governors

A Major Change may not proceed unless all required approvers have explicitly confirmed approval.

Major Changes include, but are not limited to:

- Transferring, redirecting, or reassigning the website domain, DNS records, or registrar control.
- Changing, replacing, or adding any payment processor, merchant account, financial vendor, or money-receiving platform.
- Creating or modifying any workflow that affects how funds are received, deposited, refunded, or reported.
- Establishing new third-party accounts that collect member data, payment information, or operational records.
- Any change that materially affects legal compliance, financial controls, or ownership of digital assets.
- Any action that could significantly impact chapter continuity, member access, or public-facing identity.

Documentation Requirement

All Major Change approvals must be documented by the IT Committee, including:

- Names of all approvers
- Date of approval
- Summary of the change
- Any conditions or follow-up requirements

The IT Committee may not implement a Major Change until documentation is complete.

## 12. Non-Compliance

Website-impacting changes made outside this process may be removed, disabled, or reverted by the IT Committee pending proper review.

Repeated attempts to bypass this policy may result in removal of website access or referral to chapter officers or the Board.

## 13. Recommended Standard Language for Committees

Committees should use the following standard when planning anything that touches the website:

“Any proposed change involving the B-CC IWLA website, member portal, public-facing pages, online forms, member systems, payment or money-receiving tools, vendor links, embedded content, digital integrations, or website features must be submitted to the IT Committee for review before publication or implementation.”

## 14. Policy Adoption

This policy becomes effective upon approval by the Board or appropriate chapter leadership. It applies to all committees, officers, volunteers, vendors, and administrators involved in website-related activities.

## Appendix A: Short Version for Email or Committee Communication

The IT Committee should be involved in any decision that impacts the website, member portal, public-facing pages, website features, online forms, member systems, third-party tools, vendor links, embedded content, or any process involving payments or receiving money. The website is now tied into membership, renewals, invoices, forms, payment status, reporting, and other chapter workflows, so even a simple button, link, form, or external vendor can create technical, financial, privacy, or reputational risk. Going forward, committees should submit website-related requests to IT for review before anything is published, linked, embedded, installed, or changed.