SBNC Wild Apricot Permissions Guide

Document: Permissions Structure, Rationale, and Recommendations
Last updated: December 2025

I. Overview: How Permissions Are Set Up in the SBNC System

Wild Apricot provides three main types of administrative access:

- **Full Admin**
- **Restricted Admin**
- **Read-only Admin**

SBNC uses these roles in combination with other access control tools:

- **Groups** – segment members for communications and page visibility
- **Membership Levels** – control event pricing, registration eligibility, and page access
- **Event Categories** – segment events and restrict editing access for admins (planned)

Our permissions strategy is designed to strike a balance between operational flexibility and system safety. Because we are a volunteer-run organization with frequent leadership transitions, the structure must minimize both training burden and exposure to security and data integrity risks.

II. Current Admin Role Mapping and Justification

SBNC Role	WA Admin Level	Access Setup
VP of Technology	Full Admin	Unrestricted access to all modules. Responsible for infrastructure and admin management.
President	Full Admin	Full access for emergency oversight and operational decisions.
VP of Activities	Restricted Admin	Access to Events module (all categories), view-only access to Contacts and Finances.
Posting	Restricted Admin	Limited access to Events module by category. No finance access. Cannot publish.
Event Chair	Restricted Admin	Assigned to one category only (future); can manage events in their area.
Treasurer	Restricted Admin	Access only to Finance module. No Events or Contacts access.
VP of Membership	Restricted Admin	Access to Membership module. View-only for Events and Contacts.
VP of Communications	Restricted Admin	Access to Website and Emails. View-only for Events.

This structure attempts to **minimize exposure to global data and settings**, while enabling each role to perform their duties effectively.

III. Why We Use These Roles and Tools

Each access control tool plays a specific role:

Mechanism	Purpose at SBNC
Admin Roles	Assign backend privileges aligned with board/committee responsibilities
Groups	Control access to private content and segment member lists for emails
Membership Levels	Differentiate access and pricing for Newbies, Newcomers, Extended, etc.
Event Categories	*(Planned)* Limit event editing to relevant admins; clarify calendar filters

This system allows:

- Targeted **email communication** (e.g., to Hike Group or Extended Newcomers)
- Event **visibility rules** (only Extended Newcomers see certain events)
- Controlled access to **admin modules** (e.g., Finance, Website)

IV. Outbound Communication Controls

Outbound communication (email and notifications) in Wild Apricot is influenced by:

Tool	Can Be Used To Send Emails To
Groups	Specific sets of members (e.g., Board, Event Chairs)
Membership Levels	Broad member types (e.g., all Newcomers)
Saved Searches	Filtered contacts by tags, date joined, etc.
Admin Roles	Determines who can **send** the emails, not who receives them
Event Categories	*(Indirectly)* allow limiting which event-related admins send registrant emails

SBNC Best Practice:
Use **Groups** to manage outbound communication to:

- Avoid accidental emails to full membership

- Preserve communication boundaries for roles
- Allow each VP or Chair to target only their audience

V. Current Gaps and Risks

1. **Event Categories not yet implemented**
    - All event-related Restricted Admins currently see all events.
    - No way to limit event-specific communication or editing rights.
2. **Too many admins with broad rights**
    - Risk of accidental or malicious edits to settings, emails, or financial data.
3. **No audit trail**
    - WA does not log individual admin actions.
    - Cannot trace misconfigured emails or permissions changes.
4. **Credential sharing**
    - Volunteers have occasionally shared logins.
    - Increases phishing and breach risk.
5. **Confusion around tags vs groups**
    - Tags are often misused as if they restrict access — they don't.

VI. Recommendations for Reducing Vulnerabilities

1. Implement and Use Event Categories

- Define categories for each event type: Hikes, Social, Orientation, Board, etc.
- Assign events to categories
- Restrict admin access by category to limit who can send emails and edit events

2. Audit and Minimize Full Admins

- Only the VP of Technology and President should retain Full Admin rights

- All others should be assigned specific modules as Restricted Admins

3. Stop Credential Sharing

- Enforce per-person logins
- Update login credentials during leadership transitions

4. Clarify Use of Groups vs Tags

- Use **Groups** for segmenting members for email, content access, and registration
- Use **Tags** only for filtering, not for permissions

5. Improve Admin Onboarding

- Provide role-specific training on what access is granted and what not to touch
- Use checklists and walkthroughs for new VPs and Chairs

VII. Conclusion

SBNC's permission and access model is functional but exposed. By:

- Implementing event categories
- Clarifying group vs tag usage
- Tightening admin access
- Enhancing onboarding and documentation

…we can make the system safer, simpler, and more supportive of the board and its volunteers.

This guide should be reviewed quarterly and maintained alongside the separate **Access Control 101** reference guide.

Prepared for: SBNC Tech Chairs and Board Leadership
Maintained by: Technology Committee