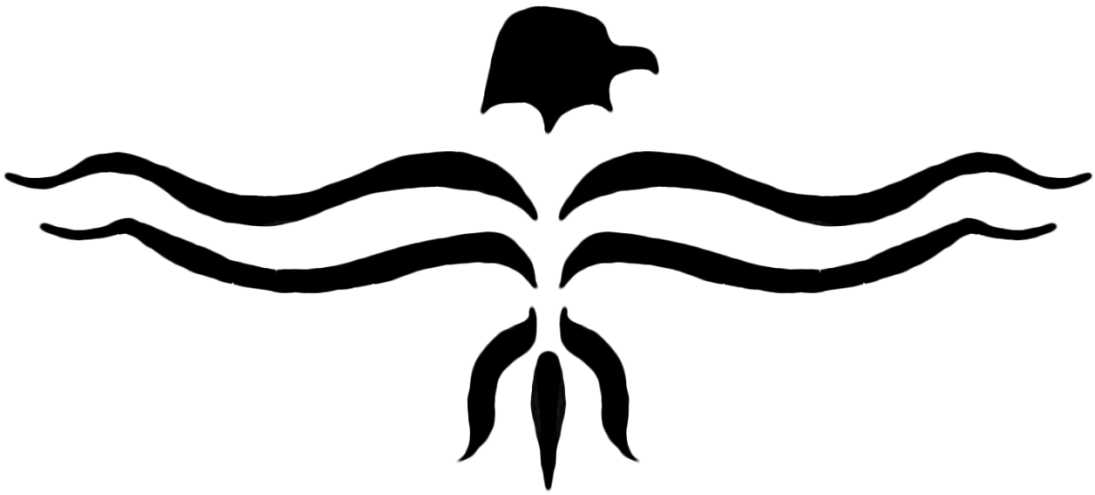

Blackhawk Ranch

Property Owners Association

Information Technology Plan

Published: May 29th 2026

Table of Contents

1. Purpose/Overview 1
2. Responsibilities 1
3. Scope 1
4. Stakeholders 1
5. Best Practices 2
6. Information Security and Data Protection 3
7. Ownership 3
8. Conflict of Interest 3
9. Reporting 3
10. Budget 4
11. References 4

Published: May 29th 2026

1. Purpose/Overview

The purpose of the Information Technology Plan is to define how the Technology Committee will manage and sustain the Blackhawk Ranch POA information technology infrastructure and tools. This includes identifying, selecting and deploying new capabilities using engineering best practices. The objectives of this committee are to enhance community engagement through the use of reliable information technology tools, provide security of sensitive information, and streamline administrative efficiency, providing recommendations to the Board of Directors for approval.

2. Responsibilities

The IT Committee serves at the direction and pleasure of the BHR POA Board of directors and will follow the polices set forth in the BHR POA Policies and Procedures. The BHR Policies and procures provides direction on budgeting, meeting standards, committee membership and administrative requirements.

3. Scope

The IT Committee has the authority to manage and sustain the following tools

- Blackhawk Ranch POA website. The BHR website is single repository for all POA related documentation and information.
- MS 365 file storage, applications, email. MS 365 provides files storage, email and MS Office applications for the board of directors, POA Members, and support functions.
- BHR Texting Service. The BHR Texting Service is a free Opt-In service used for emergencies notifications.
- GROOM Road Maintenance Application. GROOM is a Road Maintenance planning and implementation tool.
- Domain Names. Blackhawkranch.org and BHRPOA.com are registered through godaddy.com
- DNS configuration. DNS is configured within WIX web hosting platform to manage the domain name to IP Address translation for web services and email.
- Additional software, hardware or application utilized by the POA.

4. Stakeholders

3.1 Chair. The chair provides team leadership, meeting management, manages membership and communicates with the stakeholders

3.2 Team Members. Team members must possess technical skills to fulfill POA IT technical requirements. The team members and chair will work together on IT matters to ensure successful IT management and sustainment.

3.3 BHR POA Board of Directors. The Board of Directors are the primary stakeholder and approval authority of all deployed BHR POA Information Technology products.

3.4 BHR Property Owners. The Property Owners are key stakeholders of POA IT products. Tools and/or data must be available as required by BHR POA Policies and Procedures and CCIOA.

5. Best Practices

- To the greatest extent possible, the IT Committee will implement readily available commercial tools. If such tools are not available or feasible, locally developed tools may be developed.
- Lean engineering processes. The technical team will follow a lean engineering process to ensure the correct tools are selected or developed, and deployed with limited downtime. The processes will be based on Systems Engineering and Software Development Lifecycle principles.
    i. Customer needs statement. All tools, software or hardware must meet BHR POA goals and objectives. A simple needs statement highlights the business case for the stakeholders needs.
    ii. Requirements. Requirements will be derived based on the needs statement. Technical or functional requirements describe detailed features or capabilities. Nonfunctional requirements describe systems attributes like security and reliability.
    iii. Tool Selection or Design. Prior to selecting a tool, a simple trade study will be performed to ensure the best tool or hardware is selected meeting all the documented requirements. If a software tool is unavailable, the Committee may choose to develop a tool but must follow Software Development Lifecycle disciplines. Agile software development methodologies will be utilized to ensure rapid development.
    iv. Prototype. Developed tools will be prototyped and tested internally before deployment.
    v. Verification/Validation. Tool capabilities will be tested against the requirements to ensure all the requirements are met.
    vi. Test. Testing will be conducted within the committee and using a select group of people before consideration for deployment.
    vii. Approval. The IT Committee will review and approve all tools prior to review and approval by the Board of Directors.
    viii. Deploy. Develop a deployment plan to limit downtime of existing tools and to ensure a pleasant customer experience.
    ix. Sustain. A sustainment plan will be developed for all locally developed tools to ensure functionality and unplanned downtime. This includes patch management to remediate security vulnerabilities and fix software bugs.
    x. Change Management. Changes to software will be reviewed by the IT Committee prior to deployment

- Documentation. Locally developed tools will be properly documented for users and administrators use.
- Source Code. Source code will be reviewed and available to any committee member.
- Dry Principle. Avoid code duplication by using reusable components to improve code efficiency and to simplify maintenance and updates.
- File and Data Duplication. Reduce or eliminate file and data duplication to avoid version control issues, data inconsistency, storage waste and maintenance complexity.

- Training. Training will be developed for all developed software

6. Information Security and Data Protection

Implementation of Information Security practices is critical to the protection of BHR POA data, system and assets from unauthorized access, modification and destruction.

- Access Control. Each tool must have unique role-based accounts, e.g. user and administrator accounts. Unique user accounts and passwords will be used to gain access to systems. User names and passwords will not be shared.
- Password Management. Enforce strong password policies for all accounts.
- Multi-Factor Authentication. MFA will be considered to each user account.
- Least Privilege. Users will only be provided the minimum access needed to perform their duties.
- Encryption at Rest and in Transit. All sensitive data on servers and in transit over the internet or networks will be encrypted. Sensitive data includes phone numbers, email addresses, social security numbers, etc.
- Security. Tools will be secured from unauthorized access to ensure or limit infiltration of bad actors who may do data skimming, spamming, or denial of service attacks.
- Tool Management. All tools will have the capability for multiple administrator logins. In any case a tool does not have this capability, the username and password will be recorded and shared with the other IT Committee members in a secure manner or made available upon request. Transparency is essential to ensure long term viability of any implementation.
- Data Backup. Regular data backup will be preformed to ensure data integrity and prevent loss due to corruption, software or hardware failure.
- Logging. All systems will have logging available to record key system activity to include login attempts.

7. Ownership

- The BHR POA is the owner/licensee of all commercially purchased Information Technology products.
- Locally developed tools must come with, as a minimum, an indefinite license and a sustainment plan.

8. Conflict of Interest

The IT Committee must avoid conflicts of interest by not financially benefitting from products or services used by the POA. For example, the committee members may not develop and sell a product to the POA or resell a commercial product to the POA.

9. Reporting

The IT Committee will report status of all projects to the BHR POA Board of Directors as requested or during executive meetings.

10. Budget

Each year the Technology budget will be developed by the IT Committee in accordance with the BHR POA Policies and Procedures Section 400. All purchases must be approved by the Board of Directors.

11. References

- ITIL. Welcome to ITIL
- INCOSE. INCOSE - The Trusted Authority in Systems Engineering
- SDLC. Software Development Life Cycle | Microsoft Power Automate
- CIS. Center for Internet Security
- ISSA. Information Systems Security Association - ISSA International