

OVERVIEW OF PALANTE'S DIGITAL SECURITY PROCESS

Below is an overview of our full organizational digital security process. Each element of the process is accompanied by our estimate for how much coordinator and staff time that element will require.

I. INTRO AND GROUNDING SESSION – 1.5 HOURS ALL-STAFF

We facilitate a Zoom session for all staff who can attend to ensure that everyone is familiar with and has buy-in for the org digisec process we're starting together. This includes an orientation to the entire assessment organization for all staff, an introduction to the frameworks and concepts we use to think about digital security, and a participatory discussion about what safety and security mean both individually and organizationally.

II. DATA INVENTORY – 1 HOUR PARTIAL STAFF/COORDINATORS

During this Zoom session we familiarize key members of the staff with how to compile a data inventory that provides a comprehensive view of how and where the organization stores data. We answer any questions about how the data inventory should be completed and begin working on it together during the session.

III. COMPLETE DATA INVENTORY – 2-3 HOURS COORDINATORS

Working closely with process coordinator(s) from the organization, we finish compiling the data inventory. This usually involves follow-up questions and requests for clarification over email or Zoom until the data inventory is complete.

IV. THREAT ASSESSMENT SESSION – 2-3 HOURS ALL-STAFF

We facilitate a Zoom session for all staff who can attend to familiarize everyone with the threat assessment process. We begin mapping out the organization's most important data assets and identifying and prioritizing threats to those data assets. This is a longer session and will include at least 1 break.

V. COMPLETE THREAT ASSESSMENT – 2-3 HOURS COORDINATORS

Again, we work closely with the process coordinator(s) to finish compiling the threat assessment, with follow-up via email and Zoom as needed.

VI. ADDITIONAL PROJECT MANAGEMENT, COACHING, AND SUPPORT – 2-3 HOURS COORDINATORS

We usually ask follow-up or clarifying questions via email to staff member(s) acting as the coordinator for the process. Palante can support in figuring out who at the organization is best equipped to answer those questions, if it's not the coordinator(s).

VII. PALANTE RECOMMENDATIONS AND IMPLEMENTATION SUPPORT

After the portions above are complete, Palante aggregates and analyzes information from the grounding, data inventory and threat assessment.

We then provide a written report summarizing our assessment takeaways providing tailored recommendations with clear next steps to improve organization’s digital security with new policies, practices and technical solutions

Finally, Palante will work with the organization to implement the highest priority recommendations or to hand off the recommendations to other trusted services providers who already work with the organization.

TIME ESTIMATE

Group	Time (hours)
Coordinator(s)	9.5 - 13.5 (incl partial and all-staff time)
Partial Staff	4.5 - 5.5 (incl all-staff time)
All-Staff	3.5 - 4.5

ABOUT PALANTE TECHNOLOGY

Palante Technology is a worker cooperative dedicated to providing technology support to progressive, social-justice-focused organizations.