5.1 Choosing a Disclosure Policy

For those responsible for implementing the CVD process, defining a disclosure policy is an important first step. A well-defined policy makes it clear what other participants in the CVD process can expect when they engage with you and establishes good relationships between finders, reporters, vendors, coordinators, and other stakeholders.

A disclosure policy typically describes what CVD stakeholders (finders, reporters, vendors, coordinators) can expect in terms of these factors:

- **Scope** – A description of the scope of issues to which the policy applies. This scope should be as explicit as possible, especially when there are specific boundaries of concern to the organization. If a bounty is to be paid for some classes of vulnerability reports, the scope definition should clearly delineate which kinds of reports will be eligible for the bounty.
- **Exceptions** – Any exceptional conditions that may alter the typical flow of the process
- **Safe Harbor** – Should your organization choose to explicitly disavow legal retribution against reporters who otherwise follow the policy, that fact should be clearly laid out in the policy document.
- **Report quality requirements** – It's okay to require reports to meet a certain level of quality before committing to taking action on them. However, it's also useful to judiciously apply the principle of robustness here: "In general, an implementation should be conservative in its sending behavior, and liberal in its receiving behavior" [1].
- **Preferred Communication Language(s)** – If the organization has preferences for specific (human) languages for reports, the policy should specify this. That said, English is usually acceptable as a default.
- **Contact Information** – How should reports be submitted? How can you be reached?
- **Timing** – Setting expectations for response timelines of the various milestones in a vulnerability report case can be helpful too. Most important are expected time to acknowledge receipt of a report and a default disclosure timeframe if one has been defined. An acknowledgement timeframe of 24-48 hours is common for vendors and coordinators, while 45-90 days seems to be the normal range for disclosures these days. That said, we recommend that both vendors and reporters treat policy-declared disclosure timeframes as the starting point of a negotiation process rather than a hard deadline.

A few examples of vulnerability disclosure policies can be found in Appendix E.

RFC 2350 provides recommendations on how to publish information about your CSIRT and disclosure policy and procedures [2].

References