UNITED WAY OF YELLOWSTONE COUNTY
CONFIDENTIAL INFORMATION, SECURITY, AND PROTECTION POLICY

A. Statement of Purpose

United Way of Yellowstone County (UWYC) will ensure that any information which is confidential, privileged or nonpublic is protected and not disclosed inappropriately. Internal use or discussion of this information will be on a "need to know" basis.

B. Definitions

Board members, employees, volunteers and authorized representatives that have access to confidential, privileged or nonpublic information must treat the information as proprietary UWYC property for which they are personally responsible.

It is the policy of UWYC that the internal business affairs of the organization and all program participant information represent UWYC assets; which each board member, employee, volunteer and representative has an obligation to protect. This includes avoiding and preventing inappropriate disclosure of UWYC matters regarding its employees, its programs and its program participants.

No board members, employees, volunteers or authorized representatives of UWYC will release contribution data, corporate or personal, confidential agency information (such date of birth, address, credit card, background check, ACH, donor data, budgets, applications for funding, or audits to any persons other than UWYC employees, board members or volunteers. The names and addresses of UWYC campaign prospects are also considered confidential. The CEO must approve the release of all confidential information to any unauthorized parties and information designed to be shared with the community.

C. Best Practices

- During actual use, all UWYC sensitive and or private information must be continuously protected from inadvertent disclosure to unauthorized persons. It must be kept under proper control by the person using it and should not be used where it cannot be protected.
- When handling sensitive or private information in the UWYC office, special care shall be taken when visitors are present. Turn sensitive or private documents face down or use a cover sheet or place documents in a locked storage container. Never discuss sensitive or private information during telephone conversations or other communications in the presence of visitors.
- Sensitive and/or private information shall not be discussed on the telephone unless it is necessary, it is safe (closed door, no external people in office, etc.), and there is a business need to do so. Reference prior communications whenever possible to avoid information being repeated over the telephone.

UNITED WAY OF YELLOWSTONE COUNTY
CONFIDENTIAL INFORMATION, SECURITY, AND PROTECTION POLICY

- Reproduction of United Way of Yellowstone County sensitive and/or private information shall be limited and only as needed. Only make as many copies of sensitive and/or private information that are needed for a specific business function or need.
- Sensitive and/or private information shall be stored and locked in containers during non-work hours or when persons are out of office. This includes, but is not limited to background checks, blank checks, payroll information, personnel records, financial documents, and planned giving.
- Security measures shall be taken to prevent unauthorized access to sensitive information. Keys to locked containers shall always be controlled by the Finance Director and President and CEO.
- Proper disposal of sensitive and or private information shall be strictly enforced. Sensitive and or private information that requires disposal shall be shredded according to the timeline outlined on the Records Retention and Destruction Policy. Materials include drafts, work sheets, excess copies, receipts, invoices etc.
- Sensitive and private information shall not be left on white boards in conference rooms.
- Employees, Board members, committee members and other designated volunteers are expected to sign an annual attestation statement document their understanding of this policy.

D. Technology Security Guidelines:

- The server shall be stored in the locked computer room. Keys to locked doors shall always be controlled by the Finance Director and President and CEO.
- Laptop and desktop computers shall always be password protected, closed and/or off when not in use.
- Passwords will be reset quarterly.
- Passwords are never to be shared with anyone.
- UWYC files/documents should not be downloaded to personal desktop/laptop.
- Employees will participate in annual training to recognize, avoid, and report any phishing, scams, malware, and other cyber security threats. Any concerns of possible cyber security threats on personal or UWYC devices while performing UWYC work will be reported immediately.
- In the event of a lost or stolen UWYC issued device, the employee will report this to the President and CEO immediately.
- When handling sensitive or private information in a remote work location, the above guidelines apply. Only documents necessary for the employee to do their job, and that are not available electronically, should leave the office. The documents will be brought into the office on a weekly basis for filing (by the Finance Director or President and CEO) in a locked storage container.
- When handling sensitive or private information electronically, information must be submitted via encrypted email messaging.
- Electronic records with sensitive or private information will be stored in a password protected folder in the shared drive (Z:).

- Employees should log off their computers when away from their desks.
- Employees should turn off monitors at desk when working remote.