

## CONFIDENTIAL COMPANY INFORMATION

Confidential information is any information you know as a result of your BPNC employment not generally known to people outside the organization, about its business, strategies, plans, finances, operations, methods, processes, compositions, computer software/programs, research projects, product information/reports, suppliers, accounts, billing methods, and supply sources. It also includes client accounts, information, reports, finances; personal information of any person participating in BPNC sponsored or coordinated programs; and any other third party information confidentially entrusted to BPNC.

Confidential information may be in written, verbal, electronic or any other form.

### **Examples include, but are not limited to:**

- Vendor identities
- Vendor capabilities
- Non-public financial information about BPNC.
- Information about community members we serve.

Confidential information should not be revealed or discussed with family, friends, or anyone else outside the organization without prior written management approval.

An employee who improperly uses or discloses confidential information will be subject to disciplinary action, up to and including termination of employment.

The following is BPNC's Confidentiality Policy in regards to personal client information:

- When handling social security cards, do not leave them unattended while at the photocopier or whenever they are not in the owner's possession.
- Do not make extra copies of social security cards or applications. Extra copies made in error must be destroyed as soon as possible.
- After each client has stepped away, be sure to put away their paperwork so that it is not seen by the following client.
- All sensitive documents must be filed in a cabinet which is locked at all times. The key to this cabinet should be secured at all times. Examples of sensitive documents include but are not limited to social security cards, documents listing social security numbers, check stubs, benefit letters, utility bills, other personal information or forms that display personal client information.
- Minimize and do not leave open (when you walk away from the computer) the LIHEAP.NET screen, or any other computer program / internet site that may contain

personal and private client information. If you see the screen open and unattended, please close it and notify the Deputy Director of Community Services immediately.

- No sensitive documents should leave the office for any reason except to be transferred through appropriate means as defined by the program in operation.

Notwithstanding the foregoing, nothing in this policy shall prohibit or restrict you from speaking to an attorney or exercising rights that cannot be waived as a matter of law, or limits you or your counsel from lawfully (A) initiating communications directly with, cooperating with, providing information to, causing information to be provided to, or otherwise assisting in an investigation by any governmental or regulatory agency, entity, or official(s) (collectively, "Governmental Authorities") regarding a possible violation of any law; (B) responding to any inquiry or legal process directed to you individually (and not directed to the Company and/or its subsidiaries) from any such Governmental Authorities; (C) testifying, participating or otherwise assisting in an action or proceeding by any such Governmental Authorities relating to a possible violation of law; (D) discussing or disclosing information about the underlying facts or circumstances of any claim of a violation of federal, state or local law that prohibits discrimination, harassment or retaliation (for example, Title VII of the Civil Rights Act and similar state and local laws); (E) making disclosures that are protected under the whistleblower provisions of any applicable law; or (F) engaging in conduct or communications protected by the National Labor Relations Act ("NLRA"), such as assisting coworkers, former coworkers or the NLRB, or otherwise exercising your rights under Section 7 of the NLRA. Nor does this policy require you to obtain prior authorization from BPNC before engaging in any conduct described in this paragraph, or to notify BPNC that you have engaged in any such conduct.

Please take note that pursuant to the federal Defend Trade Secrets Act of 2016, you shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that: (a) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (b) is made to your attorney in relation to a lawsuit for retaliation against you for reporting a suspected violation of law; or (c) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.