OFFICE OF THE WHISTLEBLOWER OMBUDS

Sample Whistleblower Confidentiality Policy[i]

Purpose: The purpose of this document is to ensure sufficient protections for the confidentiality of sensitive whistleblower information as the [**Member office or Committee**] (hereinafter, "Office") engages with whistleblowers from the public and private sectors to support the Office's oversight work [**and constituent support functions**].

Requirements: The House Code of Official Conduct mandates confidentiality protections for whistleblower information, and House Information Security Policy requires heightened security protections for information provided in confidence or with restrictions on its use.[ii]

Information provided to the Office by a constituent, source, or whistleblower (hereinafter, "whistleblower") may fall within the ambit of this policy. As a best practice, the Office will assume that whistleblower information is sensitive and should be handled and used with caution.

Note: This Information Security Policy relates solely to information that is **not** classified. Policy and procedures for matters relating to classified material or communications are **not** contained in this document. Consult the Office of House Security for specific guidance concerning the lawful handling of classified information. Consult the Office of the Whistleblower Ombuds for guidance on the laws and processes that protect classified whistleblowing disclosures.

1. **Decision maker(s).**
   The [**Member/Chair/Ranking Member**] has responsibility for making the key decisions affecting the Office's collection, retention, and use of all information related to whistleblower matters.
2. **Principal contact.**
   The principal contact for overseeing and implementing this policy is the Office's [**insert title**].
3. **Office staff cybersecurity training requirements.**
   Personnel handling sensitive information are responsible for meeting all minimum cybersecurity training requirements in accordance with House Information Security policies.
4. **Purpose for collecting information.**
   The Office will collect information from whistleblowers to further the Office's oversight goals [**and support constituent services**]. Whistleblowers may be constituents or individuals seeking the Office's assistance with remedying misconduct or seeking assistance for reprisal they face for reporting misconduct.
5. **Intended use for the information collected.**
   Information will be collected to assess the validity and extent of the alleged misconduct; to support a decision whether to pursue, or not pursue the matter; to guide investigation and

oversight of the alleged misconduct; and to inform legislation to address the alleged misconduct. Additionally, information may be collected to support whistleblowers facing retaliation.

6. **Confidentiality protections for individuals making protected disclosures.**
   The identity of, and personally identifiable information about, an individual making a protected disclosure to the Office under federal whistleblower law will be protected from public disclosure under the House Code of Official Conduct, Clause 21. Limited exceptions exist, such as the whistleblower's advance written consent.[iii]

   Applicability of Clause 21.
   The determination of whether a disclosure is protected under a federal law is ultimately a matter of law and fact.[iv] The Office will liberally construe the application of law to the facts of whistleblower matters brought to its attention to err on the side of treating matters as falling under the protections of Clause 21.

7. **Heightened Information security protection for sensitive information.**
   Information provided to the Office in confidence or with restrictions on its use is considered **sensitive information** and will be provided heightened electronic, physical, and personnel security protections in accordance with House Information Security Policy for the Protection of Sensitive Information (HISPOL 010.0).[v]

8. **Information to be collected.**
   Examples of information typically collected follow.
   a. Involving a whistleblower.
      i. Name, age, address, phone number, title, work history, salary
      ii. Other personally identifiable information (i.e., Privacy Act)
   b. Involving their employment.
      i. Employer, job location, department, division, section, supervisors, and projects
   c. Involving their disclosure.
      i. Substance of the disclosure
      ii. Timelines of the alleged misconduct or disclosures
      iii. How the alleged misconduct came to the whistleblower's attention
      iv. Documentary evidence (i.e., emails, photos, notes of phone calls, other records)
      v. Metadata associated with documentary evidence (i.e., track-changes and author information embedded in a file, geo-location data embedded in a photo)

9. **Information considered personally identifiable or sensitive.**
   On a case-by-case basis, any or all the information identified in paragraph 8, above, may require the confidentiality protections of the House Code of Conduct and the heightened electronic, physical, and personnel security protections of HISPOL 010.0. The Office will liberally construe the boundary of which information will be protected under this policy, but as a baseline, the following will be considered **sensitive (whistleblower) information**.
   a. Identifying characteristics of a whistleblower (i.e., name, address);

b. Information relating to a whistleblower who provided information in confidence or with restrictions on its use. This may include the unique set (or subset) of facts, even without names or other commonly identifiable elements, that encompasses a disclosure of misconduct or retaliation because it may be sufficient to identify the whistleblower; and
c. Information provided in confidence or with restrictions on its use.

10. Notice and consent procedures.

a. As information is collected from whistleblowers, they will be given notice of their right to confidentiality under the House Code of Official Conduct, Clause 21. Here is a sample script of what may be said:
   - If you choose to remain confidential, the Office will respect your wishes and do everything within its power to protect your confidentiality.
   - Offices are generally prohibited from publicly disclosing your identity without your prior written consent, but there may be limitations that we will discuss, for example, surveillance technology and legal limitations.
   - So, there can be no guarantee of confidentiality. You may need to take additional precautions, such as, camouflaging your digital footprint or unique facts, having a plan for the possibility of your confidentiality being breached, and seeking experienced legal counsel.
b. Whistleblowers will be informed of the Office's confidentiality and information security practices, largely as captured in this document, and will be granted the following rights:
   i. Right to have the integrity and security of the information adequately protected;
   ii. Right to review the information in advance of its use by the Office;
   iii. Right to update the information to correct errors and remove identifiable information; and
   iv. Right to object to the use, including sharing, of the information.

11. Confidentiality and information security procedures and controls.

Whistleblower information that requires confidentiality and heightened information security protections will have the following protections:

a. All staff will be educated on their responsibility for protecting sensitive whistleblower information, including the mandate to maintain whistleblower confidentiality, in accordance with this policy, the House Code of Official Conduct, and under House Information Security Policy for the Protection of Sensitive Information, HISPOL 010.0;
b. Access is restricted to authorized staff designated as having a need to know;
c. Contractors and vendors must execute a non-disclosure agreement prior to access;[vi]
d. Electronic information will be communicated, processed, shared, and stored on official House equipment (including authorized removable media[vii]) and House-contracted technology service providers, using official House accounts;
e. Only House-approved security software and House-contracted cloud services will be used;[viii]
f. Electronic systems will be kept in compliance with House cybersecurity standards, including secure, regular automated backups, and up-to-date;

g. All electronic data-at-rest will be encrypted. This includes desktop and laptop computers, tablets, smartphones, and authorized removable media;[ix]
h. Removable media will be labeled appropriately;
i. Hard-copy information will be labeled appropriately and stored securely;
j. Electronic communications will use encryption, e.g., Signal, https://signal.org, Wickr, https://wickr.com/;
k. Hard-copy information and removable media in transit will be labeled, securely wrapped, and affirmatively tracked; and
l. Disposal of hard copy and electronic information will be done securely.[x]

12. Third party sharing.

The general prohibition, under the House Code of Official Conduct, on public disclosure of the identity of, or personally identifiable information about, a whistleblower will guide any third-party sharing of sensitive whistleblower information: Information will not be shared outside the Office without the prior, written consent of the whistleblower. However, limited exceptions will be made for the purpose of confidential consultations with House support offices, such as Office of General Counsel, the Committee on Ethics, and the Office of the Whistleblower Ombuds.

a. The Office may (notwithstanding the exceptions in Clause 21 of the House Code of Official Conduct) share sensitive whistleblower information outside of the Office under the following conditions. [xi]
    i. Prior to any third-party sharing, the terms of the third party's future use of the information, including further sharing and public release, will be negotiated. The whistleblower will be invited to participate in this negotiation or specify in advance any requested boundaries around the use of their information.
    ii. On a case-by-case basis, identifying information and metadata will be stripped out or masked before sharing. The whistleblower will be invited to inspect what is to be shared to help ensure the adequacy of this process.
    iii. Sensitive information will be encrypted when transmitted on any public access system, that is, any non-House email or platform.

13. House resources for additional support.

a. Office of the Whistleblower Ombuds, https://whistleblower.house.gov
b. House General Counsel, https://housenet.house.gov/campus/service-providers/office-of-general-counsel.
c. House Office of Cybersecurity, https://housenet.house.gov/campus/service-providers/cybersecurity
d. CAO Technology Partners, https://housenet.house.gov/technology/technology-service-providers/cao-technology-partners

[i] This document has been informed by:

1. The E-Government Act of 2002, sect. 208, P.L. 107-347, 116 Stat. 2899 (Dec. 17, 2002);
2. Office of Management and Budget Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003);
3. Fair Information Practice Principles reported in Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress, Federal Trade Commission (May 2000); and
4. House Information Security Publication, Guidelines for Determining Information Sensitivity and Security Categorization, HISPUB 010.1 (Oct. 2006).

[ii] House Code of Official Conduct, 117 H. Res. 8, Rule XXIII (Jan. 4, 2021); House Information Security Policy for the Protection of Sensitive Information, HISPOL 010.0 (Jan. 2010).

[iii] See endnote ii.

[iv] For an overview of specific whistleblower sectors and issues, see the compendium of fact sheets and Congressional Research Service reports at https://whistleblower.house.gov/fact-sheets.

[v] See endnote ii.

[vi] House Information Security Policy for the Protection of Sensitive Information, HISPOL 010.0 (Jan. 2010).

[vii] Beginning on March 31, 2021, the Chief Administrative Officer disabled access for all USB storage devices on House desktops and laptops; limited exemptions are allowed; see https://housenet.house.gov/e-dear-colleagues/important-changes-to-usb-device-and-email-auto-forwarding-rules.

[viii] See the lists at the Chief Administrative Officer's Technology Service Desk, https://housenet.house.gov/technology/software and https://housenet.house.gov/technology/cloud-services.

[ix] Consult your Technology Support Partner for more information, https://housenet.house.gov/technology/technology-service-providers/cao-technology-partners.

[x] See endnote ix.

[xi] This may also entail sharing a whistleblower's identity, after execution of a Privacy Act and HIPAA release, with a federal agency in order to obtain the release of records pertaining to the whistleblower. In cases where the whistleblower **has** requested confidentiality, the use of a privacy release to obtain documents from the agency significantly increases the likelihood that the whistleblower's identity will be revealed. In those cases, alternative channels for obtaining the information – not requiring a privacy release – should be identified and used. Consult the Office of the Whistleblower Ombuds for further guidance.