



# Guidance for Ombuds Facing Litigation Holds

## **I. Before the Litigation Hold: Best Practices from IOA's Overview of Ombuds Confidentiality (Appendix A):**

1. Ideally the reporting structure for the ombuds program should be independent from other line management functions to the greatest extent feasible within the organization. It should have an unfettered, separate reporting channel to the highest position possible within the organization, such as the CEO, or University President or senior function that is independent from any compliance or reporting channel.

2. The ombuds program should function with independence from any compliance function, any entity that administers personnel matters, the organization's legal counsel, or other function that, by definition, holds a vested interest in the outcome of issues.

3. Consistent with the requirements of standard 1.4 of the IOA Standards of Practice (Appendix B), the ombuds program should have a comprehensive, clearly written, and well-communicated and documented charter, policy, or detailed program description that clearly explains the program's structure, limitations and confidentiality expectations. Program documentation should be written with the "Wigmore Test" in mind and documentation should describe how confidentiality is an essential element to the work of the ombuds. Documentation should also clearly describe the terms and conditions for using the ombuds program, emphasizing that confidentiality is required as a cornerstone of the ombuds function and that respecting confidentiality is a condition for using the ombuds program as a voluntary resource. As a best practice, an ombuds should verbally review the program's confidentiality and limitations and ensure that each user of the program fully understands them. Such documentation will help form a basis for protecting confidentiality through the concept of an implied contract.

4. The ombuds function should be designed to meet the fundamental requirements of the IOA Standards of Practice. The ombuds function should not be vested with any policy-making, or decision-making authority regarding the issues brought to it, and should not be identified as a place to put the organization "on notice."

5. In addition to crafting program documentation that clearly outlines expectations regarding confidentiality and explains the benefits of a safe, confidential resource, (assuming the existence of an applicable mediation shield law), the program should emphasize its status as a mediation resource, which is protected by the applicable shield law.

6. The program should operate with strict physical and programmatic safeguards to ensure that confidential information is scrupulously protected, and its record-keeping functions should align with the requirements of the IOA Standards of Practice.

7. The program should develop a standard intake process for welcoming program users that includes a verbal overview of the expectations and limitations, and, as a matter of standard practice, asks the program user to state that they understand the conditions and requirements. This welcoming process should be informal and need not be legalistic or documented on a case-by-case basis, but it should be consistently used so that the practice can be demonstrated to a court if need be.

8. It is appropriate for the ombuds to work with the organization's in-house legal counsel for routine legal guidance. In situations where there is an attempt to challenge the ombuds' confidentiality or gain access to confidential information regarding a specific matter, to ensure that the program credibly demonstrates independence and full protection of confidential information (even with respect to the ombuds' own organization), the ombuds should have access to separate legal counsel that is completely independent of the organization's in-house legal function.

## **II. Sample Response Documents**

General recommended language from page 25 of the 2022 IOA Confidentiality Task Force Report (Appendix C):

1. General objections to discovery or records production requests:

a. In all cases where the organization is not on notice that the plaintiff or witness has communicated with the ombuds, adapt the general objections used for all written discovery responses, to include language that would include an objection to disclosure of confidential and/or privileged information that would cover, without specifically mentioning, the ombuds office.

b. In general, objections to written discovery responses for all cases where the organization is on notice that the plaintiff or witness has communicated with the ombuds office, include a broad confidentiality/privilege objection, as described above, and specifically mention confidentiality under the ombuds charter (and, if appropriate, any claim of ombuds privilege). The organization may also serve amended responses to specifically include this objection if it learns of possible ombuds involvement after it has first made its general objections.

2. Plaintiff's request for information about their communications with the ombuds office: Assert an objection to a specific request that: (1) the request seeks information and documents about communications with the ombuds office that are confidential (and, where appropriate, which may be privileged); (2) the organization reserves the right to supplement its response at a later time in the event a court were to rule that such communications are not confidential/privileged; (3) the organization created the ombuds office to operate independently and informally. The ombuds office functions independently of the organization and does not accept notice of claims

against the organization. and (4) to seek to obtain such information/documents, plaintiff must serve a subpoena directly upon the ombuds office at [address]. Do not provide any substantive response about any visitor communications or specific issues raised with the ombuds office.

- a. General Sample Letters: pages 27-29 of the 2022 IOA Confidentiality Task Force Report (Appendix C)
- b. US Federal: Letter Denying Request to be an Equal Employment Opportunity Investigation Witness Language can be used for any litigation hold request of a federal organizational ombuds (Appendix D).
- c. US University: Use language from IOA's "Functional Analysis: Why Ombuds Are Not Automatic Campus Security Authorities or Title IX Mandatory Reporters" (Appendix E)

### **III. Experienced Mentors / Contacts for Assistance within the Community**

- a. Ellen Miller, IOA Executive Director,

### **IV. Additional "Good Hygiene" Tips**

- a. See the Best Practices listed in the 2023 IOA Toolkit: Cybersecurity for Ombuds (Appendix F)
- b. Restrict the use of email as much as possible. Use only for scheduling conversations, not the transmittal of any case content or relevant documentation, if at all.

## **Appendix A**

**IOA Overview of Ombuds Confidentiality: Confidentiality Primer**

## **Appendix B**

### **IOA Standards of Practice**

## Appendix C

### Excerpts from the IOA 2022 Cybersecurity Task Force Report

#### **WRITTEN DISCOVERY--RESPONDING TO PLAINTIFF'S DISCOVERY REQUESTS:**

1. General objections to discovery or records production requests:
  - a. In all cases where the organization **is not on notice** that plaintiff or witness has communicated with the ombuds, adapt the general objections used for all written discovery responses, to include language that would include an objection to disclosure of confidential and/or privileged information that would cover, without specifically mentioning, the ombuds office.
  - b. In general objections to written discovery responses for all cases where the organization **is on notice** that plaintiff or witness has communicated with the ombuds office, include a broad confidentiality/privilege objection, as described above, and specifically mention confidentiality under the ombuds charter (and, if appropriate, any claim of ombuds privilege). The organization may also serve amended responses to specifically include this objection if it learns of possible ombuds involvement after it has first made its general objections.
2. Plaintiff's request for information about their communications with the ombuds office: Assert an objection to a specific request that: (1) the request seeks information and documents about communications with the ombuds office that are confidential (and, where appropriate, which may be privileged) ; (2) the organization reserves the right to supplement its response at a later time in the event a court were to rule that such communications are not confidential/privileged; (3) the organization created the ombuds office to operate independently and informally. The ombuds office functions independently of the organization and does not accept notice of claims against the organization. and (4) to seek to obtain such information/documents, plaintiff must serve a subpoena directly upon the ombuds office at [address]. Do not provide any substantive response about any visitor communications or specific issues raised with the ombuds office.
3. A request for information about the Office generally: The organization may (and it would be helpful to) provide general information regarding the function and principles of the ombuds office (such as a description of the Ombuds function from its brochure or on its website), but any such response should be coordinated with the ombuds office and/or its counsel.
4. A request for information on how visitors raise issues at the organization: Make the distinction between formal channels in the organization, which put the organization on notice, in contrast to the Ombuds office, which is informal and has no authority to receive

notice of claims against the organization. It is important in this context to cite to formal channels' policies, the organizations' code of conduct, and the ombuds' charter to substantiate these points.

5. A request for information about “all complaints” of discrimination: Assuming that a general objection has been used which objects to confidential and privileged information, the organization should be able to respond to this request without including information from the ombuds office, but the Ombuds should confirm that this is the approach the organization will use. The organization may wish to indicate in its response that its response is limited to complaints filed with formal channels who have authority to receive complaints against the organization.

#### **SAMPLE OMBUDS RESPONSES TO LITIGATION HOLD NOTICES:**

##### **1. Draft Litigation Hold Notice acknowledgement:**

Dear \_\_\_\_\_,

I acknowledge receipt of the litigation hold in the \_\_\_\_\_ matter, dated \_\_\_\_\_ and acknowledge that to the extent I have any responsive records, I will preserve them. In addition, I will suspend any normal destruction methods as to any documents potentially included in this litigation hold.

Ombuds

##### **2. Message to Risk Manager or person responsible for collecting information:**

Dear \_\_\_\_\_,

In connection. with the above referenced matter which gives rise to the Litigation Hold Notice to me, dated \_\_\_\_\_, I want to address the need for the ombuds office to protect the confidential nature of communications with visitors and as such, explain that I (as the [organization's] Ombuds) and the [organization] should assert that any information or documents relating to confidential communications with an Ombuds should not be disclosed or produced in litigation. Information sought from me as Ombuds should be considered irrelevant or, if relevant, its value is outweighed by the harm caused by breaching the promise of confidentiality. It should be argued that my testimony as Ombuds would be an unnecessary disclosure of information that is either irrelevant or available from other sources; that the plaintiff cannot demonstrate that any significant need for me as Ombuds to disclose confidential communications; and that I as Ombuds do not conduct investigations and therefore make no determination of the truth of

what may be told to me. It is also important to note that I adhere to a policy of routinely destroying any personal notes of confidential communications and as such, I routinely destroy any notes I may have created once I consider a matter closed.

In support, I have attached the [ombuds office charter or policy] which establishes the structure, function and resources of the Ombuds office at [organization] and makes it clear that the Office of the Ombuds is not part of any formal process at [organization], including but not limited to \_\_\_\_\_. In particular, I call your attention to the following important features of the office which establish the agreement between the institution, the Ombuds Office and any visitor to the Ombuds Office:

[refer to specific sections of the ombuds office charter or policy that address confidentiality and that visitor use the office based on the terms, conditions, and principles on which it was created, including not calling the ombuds to testify or produce documents in legal matters]

I also attach a written copy of the "ombuds opening script" as it was at the time of the events referenced in the Litigation Hold Notice. At the commencement of every ombuds case, I relay the information in this script orally to the visitor.

Sincerely,

Ombuds

### **3. Communication with General Counsel**

#### Privileged and Confidential Attorney Client Communication

Dear [General Counsel],

As you know, by a separate email, I responded to the Litigation Hold Notice that was sent to me in the above matter.

Because of the unique confidentiality elements of the Office of the Ombuds, however, I also want to confer with you and/or outside counsel handling this matter for (the organization) so that we can take all steps possible to preserve the confidentiality of communications with the Office of the Ombuds while collecting information responsive to your Litigation Hold Notice and in any subsequent production to the plaintiff. I believe any collection or production of documents relating to the Office of the Ombuds should be handled in a manner quite different from the collection of information from other offices or people at [the organization].

The establishment and functioning of the Office of the Ombuds is documented in [ombuds charter or ombuds policy], a copy of which I have attached. In particular, I direct your attention to the provisions of Section [\_\_\_\_] which has unique provisions:



A commitment that the Office of the Ombuds to comply with the Standards of Practice of the International Ombuds Association. [Identify applicable provisions of the Standards of Practice.]

Sections \_\_\_\_ and \_\_\_\_ of [ombuds charter or ombuds policy] expressly deal with the voluntary nature of the Office of the Ombuds and provide a defense against the production of documents from the Office of the Ombuds on the basis of privilege and contract (using the Office that was created on the basis of certain terms, conditions, and principles). Note that section \_\_\_\_ specifically provides that people who use the office will be understood to have agreed not to call the Ombuds to testify or produce records with regard to confidential communications. This same principle is embodied in section \_\_\_\_ of the Standards of Practice.

In addition to having provisions in [ombuds charter or ombuds policy] that are directly relevant to the collection and production of information relating to the Office of the Ombuds, the provisions of [the ombuds charter or policy] and other relevant information such as FAQ's appear on the Office of the Ombuds website to fairly appraise all visitors of the terms under which the benefits of the Office are made available to them. This wide publicity about the Office is further reinforced in direct communications with inquirers because it is my standard business practice to provide an introductory presentation to ALL visitors in a standard manner. Attached is a copy of the written text of the "ombuds opening script" as I have used it since \_\_\_\_\_. At the commencement of every ombuds case, I relay the information in this script orally to the visitor. Please note the section on confidentiality.

If [the organization] were to conduct its searches for electronically stored information in such a way as to intentionally include searches for confidential information from the Office of the Ombuds, any subsequent defense to prevent disclosure of this information--whether on the basis of privilege, contract, or relevance--may be unavailing on the grounds of unfairness, in the sense that [the organization] would have had access to the information but would nevertheless be trying to deprive the claimant of similar access. I understand that regardless of precautions that may be taken to protect the confidentiality of ombuds' communications, electronic discovery processes may inadvertently discover some of these communications. I believe we should discuss how the review and production of documents should be handled in this event.

Likewise, it is important that [the organization's] outside counsel be informed of these provisions and advised not to take actions that they would likely otherwise take (such as deposing the claimant and asking about the various allegations in a complaint, including ones relating to any communications with the Office of the Ombuds) for the same reasons. If a motion to compel the production of documents were to be filed by the claimant (even though prohibited by Section \_\_\_\_\_) it would be appropriate, given the assurance that the office is independent, for outside counsel to be retained to represent the unique interests of

the Office of the Ombuds and file a motion for a protective order for which [the organization could file a supporting memorandum.

I hope this email is helpful in outlining my concerns. I welcome the opportunity to meet with you and outside counsel soon to make sure that we are in agreement as to how best to protect the unique interests of the organization's Office of the Ombuds.

Thank you,

Ombuds

## Appendix D

US Federal: Letter Denying Request to be an Equal Employment Opportunity Investigation Witness  
Language can be used for any litigation hold request of a federal organizational ombuds

Dear \_\_\_\_\_,

I received your email of \_\_\_\_\_ stating that I was named as a witness in an equal employment opportunity (EEO) complaint. It is important to share the following about the ombuds role within the \_\_\_\_\_ and the Department of \_\_\_\_\_.

The \_\_\_\_\_ Office of the Ombuds is an independent, impartial, informal, and confidential resource to explore and aid in the resolution of individual and systemic issues affecting \_\_\_\_\_. It operates by a charter that was signed by the \_\_\_\_\_ Director on \_\_\_\_\_. This charter is consistent with 1) the recommendations made by the Administrative Conference of the United States (ACUS) to Congress and the President on the use of ombuds in Federal Agencies; 2) Coalition of Federal Ombudsman program and practice standards, which adopted the ACUS recommendations; and 3) International Ombudsman Association Standards of Practice and Code of Ethics.

The \_\_\_\_\_ Ombuds holds all communications with those seeking assistance in strict confidence and takes all reasonable and lawful steps to safeguard both anonymity and confidentiality. Ombuds discussion and inquiries constitute dispute resolution proceedings as defined in the Administrative Dispute Resolution Act of 1996 (ADRA), and ombuds themselves are neutrals as defined by ADRA. Confidentiality is central to ombuds practice, allowing the ombuds to create a safe space to raise issues and concerns without fear of reprisal or retribution. Consistent with the generally accepted interpretation of ADRA § 574, confidentiality attaches to communications at intake and continues until and after the issue is no longer handled by the ombuds. The Equal Employment Opportunity Commission (EEOC) Management Directive 110 also sets forth specific guidance pertaining to confidentiality of negotiations for resolution.

Given the above standards and in accordance with \_\_\_\_\_ and EEOC policies, the \_\_\_\_\_ Ombuds shall not disclose the names of inquirers or information provided in confidence to the maximum extent permitted by law, and has a duty to resist all requests for such information. Accordingly, it is not appropriate for the \_\_\_\_\_ Ombuds to appear as a witness, nor would it be useful, as I would assert and abide by the confidential nature of the communications.

If you have additional questions or concerns, you may contact me at \_\_\_\_\_.

Sincerely,

## Appendix E



### ***Functional Analysis: Why Ombuds Are Not Automatic Campus Security Authorities or Title IX Mandatory Reporters - April 2023***

Organizational Ombuds (“Ombuds”) who practice to recognized professional standards in a higher education setting provide independent, informal, neutral, and confidential services to students, faculty, and other stakeholders in support of a safe and effective campus ecosystem. Ombuds programs help address problems, conflicts, and concerns and have been a steady presence on college and university campuses for over fifty years. Today, more than seventy percent of institutions that are members of the Association of American Universities have at least one Ombuds on campus.

#### **The Ombuds Role:**

Ombuds are an independent, neutral, confidential, and informal resource to stakeholders across college and university campuses. They act as a source of information and referral, aid in answering questions, and assist in the management of conflicts and the resolution of disputes. The Ombuds office *supplements, but does not replace*, the institution’s resources for formal conflict resolution including CSAs. When Ombuds help those who seek their services (known as “visitors”) *navigate* the situation and scope of their options, they provide information about available resources, and in that capacity reassure and often remove the fear about more formal processes available, thereby safeguarding and increasing constructive reporting.

Many Ombuds act according to their institution’s charter, policy, or framework that *specifies the role of the Ombuds in that system* and whether the Ombuds will follow best practice standards<sup>1</sup>. Specifically:

Independent: An Ombuds operates independently from other organizational entities. The Ombuds exercises sole discretion over its office operations, staff, and budget;

Neutral: An Ombuds advocates *for fair and equitable processes* but remain unaligned with any individual. They are not advocates for students who make use of their services;

Confidential: An Ombuds does not disclose any information brought to its office without the permission of the individual who has confided in the office. The only exception to this

---

<sup>1</sup> In the absence of regulation, the IOA has developed *Standards of Practice* and a *Code of Ethics* to establish what best practice looks like for Ombuds. IOA also offers certification to individuals that is currently tied to where the Ombuds practices.

commitment to confidentiality is in the event that the ombuds learns of an imminent risk of serious harm to any person and there is no other reasonable option but to disclose the confidence; and

Informal: An Ombuds serves as an off-the-record resource, and *has no authority to make binding decisions, mandate policies, conduct formal investigations, or adjudicate issues for the organization*.

It is essential that community stakeholders have someone on campus with whom they can discuss matters *confidentially* without triggering an obligation to report. Parties need to know that there is a confidential, reliable resource who can provide guidance on the situation, the process, and options for reporting and/or resolution so they can make informed choices and take appropriate action. Ombuds are essential in fulfilling that role.

### **Regulatory Background:**

#### **Title IX, the Department of Education- Office for Civil Rights, and the Clery Act**

- The protection of students from sexual violence on college and university campuses has been the focus of heightened attention in recent years. The United States Office for Civil Rights of the Department of Education (OCR), the federal agency responsible for enforcement of Title IX of the Educational Amendments Act of 1972 (Title IX), has escalated its efforts to shine a light on these concerns and encourage higher education institutions to implement measures to protect students and to respond promptly, effectively, and thoroughly to reported concerns. This attention stems from the OCR's obligation to ensure non-discrimination in higher education and the proposition that sexual misconduct is a form of gender discrimination.
- Title IX and its implementing regulations, at 34 C.F.R. Part 106, prohibit discrimination on the basis of sex in admissions and recruiting, education programs and activities, and employment in educational programs. However, *the regulations do not expressly delineate an institution's responsibilities with respect to sexual violence*. Instead, *OCR has issued various "significant guidance documents"*<sup>2</sup> *that advise institutions on how the foundational anti-discrimination principles apply to sexual harassment and sexual violence*, and what institutional responsibilities arise.
- The obligation of colleges and universities to ensure student safety has also received increased scrutiny since the passage in 1990 of the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act ("*Clery Act*"). This federal statute and subsequent regulations came about as a result of 1986 rape and murder of Lehigh University student. That incident produced heightened awareness of the absence of crime-related data, and a lack of

---

<sup>2</sup> OCR issues "significant guidance documents" under authority granted by the Office of Management and Budget's Bulletin for Agency Good Guidance Practices, see 72 Fed. Reg. 3432 (Jan. 25, 2007), to "provide [federal funding] recipients with information to assist them in meeting their obligations, and to provide members of the public with information about their rights, under the civil rights laws and implementing regulations [enforced by OCR]," see April 2011 Dear Colleague Letter at n.1.

transparency regarding campus safety. Among other provisions, the regulations require colleges and universities to designate “campus security authorities” (CSAs) to report all incidents of crime brought to their attention.

- The Higher Education Act requires all postsecondary institutions in the U.S. that are participating in Title IV student financial assistance programs to disclose campus statistics on crime and security. The US Department of Education created *The Handbook for Campus Safety and Security Reporting* (“Clery Handbook”) to serve as a guide for academic institutions to help them comply with the Clery Act. Although the handbook was revised in 2016 and rescinded in 2020, it was replaced with the *Clery Act Appendix for Federal Student Financial Aid* “Appendix”.

### Changing Law and Guidance re: Who Should Report?

Over the past several years, Title IX, Title IX guidance, and Clery Act guidance has changed regarding who should be required to report sexual harassment and sexual violence. The following reflects this evolution:

#### *White House:*

- 2014 White House Task Force to Protect Students From Sexual Assault:

The Task Force emphasized the importance of providing victims of sexual violence with confidential resources for consultation, advice, and support. The report noted that victims of a sexual assault “want time and privacy to sort through their next steps,” and that having a “confidential place to go can mean the difference between getting help and staying silent.” The report goes on to state that “on-campus counselors and advocates can talk to survivors in confidence,” citing guidance from the U.S.

Department of Education <sup>3</sup>.

#### *Title IX:*

- In 2014, OCR, in its Q and A guidance following the Department’s 2011 Dear Colleague Letter, discussed notice and defined “responsible employee” as follows:

An institution is deemed to have *knowledge, or be on notice*, if a “responsible employee” knew or, in the exercise of reasonable care, should have known about alleged sexual harassment or violence. Accordingly, institutions must require “responsible employees” to report incidents of sexual harassment or violence to the Title IX Coordinator or other designated officials.

---

<sup>3</sup> Although the report did not explicitly identify the campus ombuds as one of those possible confidential resources, as noted above, Ombuds provide victims of sexual violence with confidential resources for consultation, advice, and support.

- In 2020 when Title IX regulations were revised, it limited the ways in which an institution “knows or reasonably should know” to the Title IX coordinator *or an “official with authority to institute corrective measures.”*
- May 2022: A notice of Proposed Rulemaking was issued to consider proposed amendments to Title IX. IOA made technical suggestions to the proposal that was supported by a bipartisan congressional letter to the Department of Education that stated:

“As proposed, the definition of confidential employee could mistakenly be limited and should be clarified. We understand the International Ombuds Association has filed non-partisan, technical comments that address clarifications around the definition and encourages the Department not to restrict the number of employees that can be deemed as confidential--particularly those such as ombuds that already serve effectively on many campuses. These clarifications ensure confidential resources and mandated reporters alike are clearly and effectively identified as “survivor/complainant-supporting” and “respondent-supporting.””

#### *Clery Act:*

- In 2016, the Department of Education Federal Student Aid Office revised the “Clery” Handbook to define CSAs based on a *functional employee analysis* noting:

CSA designation should be based on an analysis of the function involved: “To determine specifically which individuals or organizations are campus security authorities for your institution, consider the function of that individual or office.” (Emphasis in the original.) Despite the articulated standard of functional analysis, the Handbook lists “an ombudsperson (including student ombudspersons)” as an example of individuals “who generally meet the criteria for being campus security authorities.” Specifically, on page 4-3 it states:

Examples of individuals (outside of a police or security department) who *generally* meet the criteria for being campus security authorities include.... an ombudsperson (including student ombudspersons) <sup>4</sup> .

- In October 2020, the U.S. Department of Education Federal Student Aid Office rescinded the 2016 Clery Act Handbook for Campus Safety and Security Reporting noting:

There had been *no change to either the statute or the regulations prior to 2016* and the Handbook “*expanded the definition of a CSA to include individuals on campus who should likely not be designated so under a strict interpretation of the regulatory framework.*” And “the 2016 edition took an expansive view of the phrase “*significant responsibility for student and campus activities*” found at 34 CFR

---

<sup>4</sup> The Department of Education has noted this reference was added to address those ombuds who may have other functional responsibilities that would require the classification as a CSA. The Department continues to stress the importance of a functional analysis to fully understand the role the Ombuds plays. For Organizational Ombuds who practice to standards, a functional analysis will reveal they do not meet the criteria to be classified as CSAs or mandatory reporters, as further discussed below.

668.46(a) ). As a result, it *captured groups of individuals who did not have “significant responsibility.”*

- In 2020, the *Clery Handbook* was replaced with the *Clery Act Appendix for Federal Student Financial Aid “Appendix”*. The Appendix provides clarity re: CSAs and notes:

While not defined in the statute, regulations provide that CSAs include: (i)

campus police or security department personnel;

(ii) individuals with security-related responsibilities; and

(iii) individuals or organizations identified in institutional security policies as an individual or organization to which students and employees should report criminal offenses.

- The definition at § 668.46(a)(iv) states that a *CSA also includes an official “who has significant responsibility for student and campus activities, including, but not limited to, student housing, student discipline, and campus judicial proceedings.”*
- The Department *will defer to an institution’s designation of CSAs as authoritative* and provide any technical assistance necessary to work with institutions to help ensure proper identification and notification of CSAs consistent with the regulations. The *regulations do not require that an employee with minimal responsibilities for student and campus activities necessarily be considered CSAs* .

On a case-by-case basis, *institutions may apply the regulations to not designate CSA responsibilities for Clery Act reporting purposes to an individual* . Individuals determined not to have significant responsibility for student and campus activities may, in some cases, include those individuals who, for example, have irregularly scheduled duties or duties that are not part of an employee’s primary job description. If paragraphs (i)-(iii) of the definition of CSAs are not applicable, institutions should focus on the “significant responsibilities” of an employee when determining whether that employee is a CSA for Clery purposes. *Note that a CSA for Clery purposes will include employees who meet the definition of “any official...who has the authority to institute corrective measures” for Title IX purposes under 34 CFR 106.30(a).*

The Department’s most recent guidance made it clear that it is *up to an institution to identify which individuals are CSAs* and *it is beyond the Department’s authority to disagree with that reasonable determination*. The memorandum from the Department, and the Appendix accompanying it, make it clear that this guidance, just like the guidance in the Handbook, is just that— *guidance--not a regulation and has no force of law* .

### **Why Ombuds Do Not Need To Be Classified As CSAs or Title IX Mandatory Reporters**

As noted above, Title IX and Clery Act guidance has evolved since 2014. Even the Department of Education recognizes the value of Ombuds who practice to standards and the importance of doing a



functional analysis to determine that Ombuds are not “responsible employees” and are not “officials with authority to institute corrective measures.” Even under former guidance using the “functional analysis” test, Ombuds who practice to IOA Standards are not “officials of their institution” and do not have significant responsibility for student and campus activities.

Currently, the regulations do not require that an employee with minimal responsibilities for student and campus activities necessarily be considered CSAs. Institutions are required to conduct their own reasonable analysis and can self-determine the offices and employees that should be classified as CSAs. Current guidance notes that this determination should be viewed as authoritative by the Department of Education.

Although Ombuds are not CSAs, they play a *significant* role. They provide a safe and confidential resource to victims, an important goal as noted by the 2014 White House task force. Although they are informal, they are a critical part of the service puzzle, helping victims get to the right office to make a formal complaint.

### **Collateral or Dual Role Ombuds:**

Most Ombuds solely act in the capacity of an Ombuds. However, there are some institutions that ask their Ombuds to wear multiple hats and perform roles beyond that of the Ombuds. IOA appreciates that these “collateral” or “dual role” ombuds *could* be classified as CSAs under an institution's own functional analysis. The current process requiring the institution to assess the roles of their employees *adequately* addresses these dual-role employees. The exception should not drive the rule. The standard embodied in the current regulations both fairly applies the law and prevents properly structured programs from being considered CSAs and/or mandatory reporters.

### **About IOA:**

The International Ombudsman Association (IOA) is a professional association committed to supporting organizational ombuds worldwide. The association's members help others safely navigate conflict and change in corporations, educational institutions, non-profit organizations, government entities, and non-governmental organizations across the globe.

For more information, contact IOA Executive Director Ellen Miller at 619.738-3923 or [emiller@ombudsassociation.org](mailto:emiller@ombudsassociation.org).

## Appendix F

### 2023 IOA Toolkit: Cybersecurity for Ombuds

In 2021, IOA convened a special Task Force to explore issues related to technology and provide guidance on how best to protect the confidentiality of your communications and operations. The Task Force report addresses a variety of issues relevant to practicing organizational ombuds and:

- Identifies suggested questions concerning privacy and ombuds practice for discussion with IT professionals in your organization
- Addresses records maintenance and retention guidance for ombuds
- Includes a Privacy Policy Guide
- Provides Guidance on ombuds confidentiality re: electronic records and litigation discovery
- Offers a sample ombuds responses to Litigation Hold Notice

#### **Best Practice Recommendations:**

The report includes a series of best practice recommendations, many of which were shared at IOA's 2022 Annual Conference:

##### *General:*

1. Draft cybersecurity protocols and policies for your office
2. Hold staff trainings on cybersecurity best practices
3. Designate a cybersecurity contact person on your team
4. Explore insurance to cover potential damages
5. Utilize software platforms that ensure data security (e.g. ISO 27001 compliant)
6. Understand your compliance obligations to relevant laws and regulations
7. Tailor access rights to all data, so you know who has access to what
8. Update and patch your software and hardware
9. Secure your local software, hardware, and network

##### *Ongoing:*

1. Make cybersecurity policies, responsibilities, and protocols explicit
2. Update your policies and procedures based on changing circumstances and user feedback
3. Maintain access control rules (e.g., monthly change of password, limited time of access to documents, automated logout from shared platforms)

4. Monitor vulnerabilities by setting up instant alerts for unauthorized access
5. Stay alert for red flags (e.g., cloned emails, suspicious attachments/links)
6. Report any attack or intrusion immediately
7. Keep track of where your data goes throughout all interactions with visitors
8. Conduct periodic data backups
9. Encrypt sensitive information, both in transit (over the internet) and at rest (on your drive)
10. Avoid using free service providers (for email, data transfer, antivirus scanning)
11. Select settings that protect the security of your video conferencing sessions
12. Limit copies to portable devices (e.g., USBs, mobile phones, external drives)
13. Control all access to hard copies of data
14. Use privacy screens and webcam covers

#### *After Meetings with Visitors:*

1. Return or destroy any physical documents with sensitive data
2. Get a final security report from your software platform confirming that personally identifiable information (PII) has been deleted/anonymized
3. Encrypt or delete any archived information on your hard drives

#### *Protecting your Online Identity:*

1. Create a confirmed profile on social media (so no one can pretend to be you)
2. Disclose close relationships reflected on social media to avoid challenges to your impartiality
3. Audit and prune your social networks
4. Select safe private messaging tools
5. Use non-public chat integrated into secure online platforms whenever possible
6. Think before you click to avoid phishing attacks through social media

#### **Other Ideas to Consider:**

- Ask your IT department to do a cyber audit, and educate them about the uniqueness of your role so if a litigation hold is requested, they understand you are unique.
- Consider using calendar software that is not used in your organization (i.e. Google) to schedule meetings. Make sure the calendar is not synced with your organization's Outlook calendar.
- Use Free scheduling options to allow visitors to schedule directly and encourage that they do not use their work email to confirm the meeting. Calendly allows people to schedule meetings directly, as does Doodle. In Calendly, you can even set up multiple options but only turn on one option at a time to maintain free status.
- Purchase an independent Zoom account for your office. The Zoom information can be automatically synced to both your Calendly and Google Calendar.

- If your office uses Microsoft Teams to hold virtual meetings with visitors, be sure to change the settings per the [instructions provided by Microsoft](#) and use a single setting change to turn off 'working with' feature under 'disable group.' A security group should be created to specify the group for which the feature will be disabled.
- When software or user agreements are updated, you will receive an email. Use this prompt as an opportunity to go into settings to see if anything has changed that could impact your ability to maintain confidentiality.

**Other Resources to Assist:**

International Ombuds Association [2021 Confidentiality \(in Cyberspace\) Task Force Report](#)  
November, 2011 [Ombuds in Cloud of Exabytes--Understanding the Ombuds' Digital Trail](#), Craig B. Mousin,  
DePaul University

If you have questions related to these issues, please reach out to [IOA's Executive Director](#).