**University of California, Berkeley**

**Issued:**

**Effective Date**  *[UCB Seal Here]*

**Supersedes:**

**Next Review Date:**

**DRAFT Procedures**

for

**Privacy and Online Monitoring**

including

**Campus Monitoring Norms** and **Privacy Balancing Process**

Responsible Executive: Chief Ethics Risk and Compliance Officer

Responsible Office: Campus Privacy Office

Contact: Campus Privacy Officer, privacyoffice@berkeley.edu, privacy.berkeley.edu

This document defines implementation procedures to meet requirements of the UC Berkeley Policy on Privacy and Online Monitoring.

# Section A. - Norms and Notice

## A.1. Campus Monitoring Norms

The following Monitoring Practices are established standard practices widely accepted by the UC Berkeley Campus. Meaningful notice to users of these standard practices, as well as exceptional practices is required. These Monitoring Practices generally **do not require** a Privacy Balancing Process.

[Under Development] – see Appendix C

## A.2. The Monitoring Practice Inventory

The Monitoring Practice Inventory template in Appendix A provides the standard campus format for documenting Monitoring Practices to submit to the Information Risk Governance Committee (IRGC) and Academic Senate Committee on Computing and Information Technology (CIT). It includes:

* Method of monitoring and implementation status (e.g., proposed, existing)
* Summary
* Purpose
* Data Examined/Collected and retention period
* Recommendations (source) (for recording campus input on the monitoring practice)

The format of notice to users may differ from the Monitoring Practice Inventory.

# B. Privacy Balancing Process

The Privacy Balancing Process outlines the required analysis and approval process for proposed Monitoring Practices that deviate from Campus Monitoring Norms.

## B.1. Privacy Balancing Analysis

As minimum considerations for the UC Berkeley Balancing Process for Monitoring Practices, monitoring units must analyze and document in a Balancing Analysis the following factors[[1]](#footnote-1):

#### B.1.1. Utility:

The Balancing Analysis must document the purpose for monitoring and an estimate of current and future utility. Privacy Objective: Establish the value of monitoring or not monitoring to enable determination of whether the proposed course of action is sufficiently compelling to justify the privacy impact.

#### B.1.2. Alternatives:

The Balancing Analysis must consider alternative means of accomplishing the documented purpose, and the relative efficacy and privacy impact of the alternative approaches. Privacy Objective: Evaluate alternatives to monitoring practices that give deference to the privacy of individuals without unduly constraining other institutional operational needs.

#### B.1.3. Scope:

The Balancing Analysis must consider and document the scope of monitoring and the privacy interests of groups impacted by the monitoring. Privacy Objective: Segment and apply monitoring according to risk and privacy interests.

#### B.1.4. Use Cases:

All Monitoring Practices and uses of data collected by those Monitoring Practices shall be restricted to the use cases documented in the Monitoring Practice Balancing Analysis and must consider and document the privacy impact generally and, at a minimum, in each of the following separate categories, and also document actions that will be taken to mitigate privacy impact. Privacy Objective: Ensure that privacy is appropriately evaluated for all uses of monitoring data.

##### B.1.4.a. Operational Use:

The planned routine operational use(s) for monitoring must be defined and described in the Monitoring Practice Balancing Analysis.

##### B.1.4.b. Non-Routine Use:

Non-Routine but anticipated uses of monitoring data beyond Operational Use must also be articulated in the Monitoring Practice Balancing Analysis for review and approval. Escalation procedures to document and obtain approval for non-routine use in order to prevent routinization of such use must be specified, (e.g.,

Prior to accessing monitoring data for a Non-Routine Use the responsible monitoring party must declare the Non-Routine Use by notifying the Campus Privacy Officer (CPO) at PrivacyOffice@berkeley.edu; or

Prior to accessing monitoring data for a Non-Routine Use, the monitoring party must obtain consent or ECP non-consensual access approvals)

Non-Routine access must be logged and reported to IRGC annually. If the CPO disagrees with a non-routine use of data, escalation to IRGC for review and determination of binding principles for continued use of data is required.

##### B.1.4.c. Required Legal Disclosure:

Disclosure as required by and consistent with law, e.g., in response to a valid subpoena, court order, public records request[[2]](#footnote-2), or national security letter.

##### B.1.4.d. Significant and Exigent Circumstances:

Other uses and disclosures in significant and exigent circumstances with IRGC approval and with reliable evidence that failure to act would result in significant bodily harm or significant property loss. For time-sensitive needs, access may be granted pursuant to Campus procedures for non-consensual access established under the Electronic Communications Policy.

##### B.1.4.e. Internal Abuse

Misuse of the data within the monitoring unit.

##### B.1.4.f. Unauthorized Disclosure

Accidental disclosure of the data such as via unauthorized access to systems holding the monitoring data (e.g., hacking, theft, inappropriate security configurations.)

#### B.1.5. Least Perusal:

Privacy Objective: Employ the least invasive access to data necessary for meeting stated objectives. This favors automated analysis over manual perusal when possible.

##### B.1.5.a. Data Element Specification:

Each element of examined and retained data must be specified in the Monitoring Practices Balancing Analysis.

##### B.1.5.b. Metadata:

Balancing Analysis must include metadata, as the distinction between data and metadata is not valid in a privacy context. Balancing Analysis must assume all available data collected can be combined and correlated.

#### B.1.6. Least Disclosure:

Privacy Objective: Disclosure of monitoring data will be minimized to the least amount necessary for meeting stated functional objectives.

##### B.1.6.a. Disclosure to Partners Outside of Monitoring Unit:

When disclosing data to partners, the unit that is granted permission to monitor by IRGC is responsible for establishing and enforcing agreements to ensure that data handling practices comply with this policy and IRGC approved practices. The monitoring party is responsible for educating data recipients on data handling principles (e.g., least perusal, least disclosure, use restriction, etc.). This includes data in tickets and emails sent out for incident notification that collect in mailboxes and tracking systems.

* + 1. Binding contract provisions must require that vendor activity protect privacy and comply with campus monitoring requirements and conditions.
		2. Vendor's use of data must be limited to UCB benefit and no vendor data storage unless absolutely necessary for UCB benefit and only with IRGC approval.
		3. Any external legal (e.g., law enforcement, including UCPD, or public records) requests for data must be referred to UCB Office of Legal Affairs for review of the request’s validity. Other requests must be reviewed by the Privacy Office.

##### B.1.6.b. Disclosure Escalation Path:

When monitoring identifies situations requiring disclosure (e.g., security incidents) the monitoring party is required to first contact the concerned individual(s) unless otherwise defined and justified in the Monitoring Practice Balancing Analysis. Depending on the urgency of the situation, if the individual is not known, not available, or not responsive, the monitoring party will contact the next closest identified contact as defined in the Monitoring Practice Balancing Analysis.

#### B.1.7. Minimal Retention:

The Monitoring Practice Balancing Analysis must specify the retention period for each element of retained data. Privacy Objective: Data is retained only as long as needed to meet stated objectives (i.e., shorter is better: if keeping for X amount of time, must have a justification why X/2 is not sufficient.) Data stored is data that can be misused or compelled to be disclosed.

#### B.1.8. Data Security:

The Balancing Analysis must validate that units conducting monitoring have a documented and resourced plan for securing data, training staff in the proper use and handling of data, and applying strong sanctions for misuse or failure to follow handling procedures. Privacy Objective: Collected data must be protected from inappropriate and unapproved access and use.

#### B.1.9 Transparency and Accountability

##### B.1.9.a. Notice

Each unit conducting Monitoring Practices must publish general information about their Monitoring Practices to their users, and submit to IRGC the planned and final location and text of this notice for review and approval.

##### B.1.9.b. Reporting

In addition to notifying privacyoffice@berkeley.edu prior to any non-routine access to monitoring data, units conducting monitoring must keep records of all non-routine access and submit an annual report of this information to IRGC.

##### B.1.9.c. Compliance

Each Monitoring Practice Balancing Analysis must define procedures for ensuring ongoing compliance with this policy and the approved Monitoring Practices.

## B.2. Governance and Approvals:

Monitoring Practices falling within Section II of the Privacy and Online Monitoring Policy require transparent review and documented approval by

1) IRGC-Managed Campus Vetting,

2) Provisional Approval or

3) Expedited Review

to ensure the practices are consistent with the privacy values of the Campus, and that the appropriate balance between autonomy and information privacy and other Campus obligations and priorities is maintained. The approval process will involve review of the Balancing Analysis to deliberately evaluate what and how monitoring data may be collected, reviewed, used, and retained.

### B.2.a. IRGC-Managed Campus Vetting

The campus Information Risk Governance Committee (IRGC) is the established body for managing the Balancing Process, including prioritization of online monitoring practices for review, conducting stakeholder consultation and campus review, and granting final approval. IRGC serves as the “Campus Privacy and Information Security Board” described in the UC Privacy and Information Security Initiative (PISI) report.

#### B.2.a.i. Stakeholder Consultation

The Balancing Process requires consultation with students, faculty and staff, including the following stakeholders or their designees:

1. Information Risk Governance Committee (IRGC) with advice from the Campus Information Security and Privacy Committee (CISPC)
2. Joint Committee on Campus Information Technology / COMP Academic Senate committee
3. Chair of the Academic Senate
4. President of the Associated Students UC
5. President of Graduate Assembly
6. Additional constituents as identified by IRGC

#### B.2.a.ii. Open Review and Comment Period

The Balancing Analysis for a proposed Monitoring Practice will be announced and made available to the campus community for review and comment for at least three-weeks (not including academic breaks). The Balancing Analysis will be available for public review unless the monitoring unit justifies to IRGC the need for limited distribution.

The Campus Privacy Officer will collect, review, and responded to feedback. The Joint Committee on Campus Information Technology (faculty advisory committee jointly appointed by Academic Senate and the Chief Information Officer) will adjudicate on comments received.

### B.2.b. Provisional Approval

#### B.2.b.i. Time-Sensitive Circumstances

Monitoring units may request to operate provisionally with approval from the IRGC Provisional Approval Committee if monitoring is deemed necessary before a full IRGC-Managed Campus Vetting process can be conducted. The Committee may decline to provide a provisional decision, sending the request forward for full IRGC-Managed Campus Vetting instead.

The IRGC Provisional Approval Committee consists of:

* Campus Privacy Officer (CPO),
* Chief Information Security Officer (CISO),
* Cyber-risk Responsible Executive (CRE), and
* IRGC Co-sponsor: Chief Information Officer (CIO), and
* IRGC Co-sponsor: Associate Chancellor (AC)

Provisional approval requires notification to and attempt to obtain consultation from all Provisional Approval Committee members. However, approval by majority (any three members) is sufficient for provisional operation. If any Provisional Approval Committee member disagrees with the provisional decision, the member can prioritize a full IRGC-Managed Campus Vetting.

#### B.2.b.ii. Established Monitoring Practices

Monitoring Practices established in practice prior to approval of this policy may continue to operate provisionally until IRGC-Managed Campus Vetting. Explicit IRGC Provisional Approval is not required in this instance.

###

### B.2.c Expedited Review

The following monitoring scenarios are eligible for expedited review and exempt from the IRGC-managed Campus Vetting Process (defined in section B.1.) unless otherwise identified by the Campus Privacy Officer or IRGC as having significant privacy impact. Units conducting these Monitoring Practices must still comply with the remaining procedures required by the Privacy and Online Monitoring Policy, including conducting a Balancing Analysis (A) and submitting a Monitoring Practice Inventory (C) to the privacyoffice@berkeley.edu.edu, and Transparency (D).

The Campus Privacy Officer will consult with IRGC supporting committees and respond to Expedited Review requests within three weeks with a review determination or a time extension.

#### B.2.c.i. Meaningful Choice and Individual Consent

When individuals have meaningful choice regarding Monitoring Practices, and explicit and narrowly defined consent is obtained from individuals subject to those Monitoring Practices, those Monitoring Practices are eligible for expedited review. For example, if a service provider offers an optional monitoring service to which campus users may elect to subscribe (not required by job description or department membership, etc.) and the monitoring practices are defined explicitly to the individuals who may choose to participate or not, that monitoring practice is exempt from IRGC-Managed Campus Vetting.

#### B.2.c.ii. De-identified Data

If monitoring does not include information that identifies an individual, there is no reasonable basis to believe that the information can be used to identify an individual, and the monitoring party and anyone to whom the data is disclosed attests to the privacyoffice@berkeley.edu that the data subjects will not be re-identified and the data will not be joined with other identified data, those Monitoring Practices are eligible for expedited review.

#### B.2.c.iii Aggregate Data

Monitoring of data in aggregate form is eligible for expedited review when information pertaining to individuals is sufficiently obfuscated. Even when not personally identifiable, aggregate data merits Expedited Review to evaluate potential negative impact, e.g., keeping track of what websites get the most hits on campus (DNS lookups) could chill free inquiry.

#### B.2.c.iv. Security Monitoring of Highly Sensitive Data

When the University is the record holder for highly sensitive institutional data, the institution has a heightened responsibility to protect such data from unauthorized access. The University recognizes that online monitoring can have negative privacy impacts, however, if the University already stores and has access to such data, monitoring conducted by the University to protect the confidentiality of that data generally does not materially increase privacy risks. Therefore, monitoring data traffic to or from PL2 (highly sensitive) data systems for the purpose of protecting the confidentiality of that data is eligible for Expedited Review under the following conditions:

##### (a) Monitoring scope:

a. Proposed monitoring is restricted to activity on networks or institutional or privileged access devices registered as handling Protection Level 2 (PL2) data (as defined in the Berkeley Data Classification Standard, collectively, “PL2 systems”) *and*

b. The PL2 systems are University administrative systems handling records for which the University is the Record Holder (i.e., creator or intended recipient of the communication, as defined by the Electronic Communications Policy). Such systems include Berkeley Financial System, Human Capital Management, Student Information Systems, Central Authentication System, Financial Aid, Electronic Health Records, etc. *and*

c. Proposed monitoring does not apply to email and document storage systems where there is permissible incidental personal communication, or non-administrative records.

##### (b) Monitoring purpose:

a. Proposed monitoring is intended to protect data from a compromise of confidentiality, *and*

b. Secondary uses of collected data (other than for the protection of confidentiality described in the monitoring proposal) are prohibited, except when required by law or with authorization through the Electronic Communications Policy non-consensual access approval process.

### B.2.d. Review Feedback

The Campus Privacy Officer is responsible for providing notification and feedback regarding the outcomes of monitoring practice reviews to affected units.

### B.2.e. Exceptions

Any deviation from the requirements defined in this policy requires explicit and documented approval by the IRGC.

# Appendix A: Monitoring Inventory Template

[Unit] Monitoring Practices Inventory

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Method (implementation status) | Summary | Purpose | Data Examined/Collected; Retention Period | Recommendation\* (source) |
| *Example:**1. Central Authentication Audit (new)* | *CalNet login attempts associated with geographic location.* *Baseline patterns of systems and user authentication behavior*  | *Rule-based alerts for geographically dispersed simultaneous logins and excessive failed logins.**Detect anomalies from baseline behavior to identify potential security compromises.* | ***All*** *CalNet authentication attempts correlated with geographic location* *For PL2 (critical) assets and and users who access those assets: baseline authentication behavior (patterns)** *1 year retention*
 | *Recommend Approval* *(CISPC, CPO, CISO)* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

\*CISPC: Campus Information Security and Privacy Committee (advisory to IRGC)

CPO: Campus Privacy Officer

CISO: Chief Information Security Officer

# Appendix B: Balancing Analysis Template

[Unit Name]
Monitoring Practice Balancing Analysis:

[Monitoring Practice]

Responsible Executive:

Responsible Office:

Contact:

Document Distribution: *[Public, Campus, Other] (include justification if public posting is not recommended)*

This document inventories the Privacy Balancing Analysis required by the UC Berkeley Privacy and Online Monitoring Policy for online activity monitoring conducted by *[unit]*.

**Description:** *Describe the proposed monitoring practice.*

**Privacy Balancing Analysis**

**(per Privacy and Online Monitoring Policy requirements section I.C.)**

|  |  |  |
| --- | --- | --- |
| # | Factor | Assessment |
| 1 | **Utility:***Purpose for monitoring and estimate of current and future utility* |  |
| 2 | **Alternatives***Alternative means to accomplish the documented purpose, and the relative efficacy and privacy impact of the alternative approaches* |  |
| 3 | **Scope***Scope of monitoring, how the utility and privacy impact change if scoped differently* |   |
|  4 | **Use Cases*****All uses of data collected by this Monitoring Practices shall be restricted to the use cases documented below****.* ***Document the privacy impact*** *generally and in each of the use cases,* ***and******mitigations*** *that will be taken to reduce privacy impact:* |
|  | **General Privacy Impact** |  |
| 4a | **Operational Use:** *Planned routine operational use(s)* |   |
| 4b | **Non-Routine Use:***Non-Routine but anticipated uses.**Escalation procedures to document and obtain approval for Non-Routine use in order to prevent routinization. If data includes “electronic communications” escalation process must meet ECP requirements.* |  |
| 4c | **Required Legal Disclosure:** *As required by and consistent with law e.g., in response to a valid subpoena court order, public records request or national security letter* |  |
| 4d | **Significant and Exigent Circumstances**:  |   |
| 4e | **Internal Abuse***of the data within the monitoring unit* |  |
| 4f | **Unauthorized Disclosure** *e.g., unauthorized access to the systems holding the monitoring data* |  |
| 5 | **Least Perusal***a. Data Element Specification**(each element examined and retained, including**b. Metadata**Least invasive access to data necessary for meeting stated objectives: automated analysis over manual perusal when possible* |  |
| 6 | **Least Disclosure:** *Planned disclosures minimized to the least amount necessary for meeting stated objectives***a. Disclosure to Partners Outside of Monitoring Unit****b. Escalation Path***First contact concerned individual(s) unless otherwise defined and justified. Further escalation depending on urgency* |   |
| 7 | **Minimal Retention:** *retained only as long as needed to meet stated objectives* |  |
| 8 | **Data Security** *documented and resourced plan for securing data, training staff in the proper use and handling of data, and applying strong sanctions for misuse or failure to follow handling procedures* |  |
| 9 | **Transparency and Accountability** |
| a | **Notice***(Planned) location and text of general information about Monitoring Practice published to users* |  |
| b | **Reporting***Procedures for notifying privacyoffice@berkeley.edu prior to any non-routine access to monitoring data. Procedures for keeping records of all non-routine access and for submitting an annual report of this information to IRGC.* |  |
| 9c | **Compliance***Procedures for ensuring ongoing compliance* |  |

# Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Modified by  | Description |
| 2/21/2017 | DRAFT1.0 | Lisa Ho | Extracted from Privacy and Online Monitoring Policy v1.6 |
| 6/26/2017 | Draft 1.1(in progress) | Lisa Ho | Revisions per campus comments and Policy v1.9 |

1. The Privacy Balancing Analysis Factors were established based on information security monitoring use cases and reflect widely accepted privacy conventions found in the [Fair Information Practice Principles (FIPPs)](http://www.nist.gov/nstic/NSTIC-FIPPs.pdf). As the Campus applies this process to additional use cases, the Balancing Analysis Factors will be revised as needed after appropriate Campuswide review and vetting. [↑](#footnote-ref-1)
2. In responding to Public Records Request, the campus must balance the competing interests of (a) providing access to records about how public business is conducted, against (b) protecting the rights of privacy of an individual whose information may exist in those records. The Balancing Analysis should include considerations for such balancing.

 [↑](#footnote-ref-2)