[Unit Name]  
Privacy Balancing Analysis:

[Monitoring Practice]

Responsible Executive:

Responsible Office:

Contact:

This document inventories the Privacy Balancing Analysis required by the UC Berkeley [Privacy and Online Monitoring Policy](https://berkeley.app.box.com/file/169899416879) 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 | **Data Element Specification**   1. *List each element examined or collected (include metadata).* 2. *Specify retention period.* |  |
| 5 | **Use Cases**  **Describe all intended uses of the monitoring data:**  **a) Operational Use Cases:**  *Planned routine operational use(s)*  **b) Non-Routine Use Cases:**  *Non-Routine but anticipated uses. Detail the accounting procedure to prevent non-routine use from becoming routine (e.g., notify privacyoffice@berkeley.edu prior to use)*  ***Only these described uses are allowed. All other uses are prohibited unless approved through the escalation procedures defined below.*** |  |
| 6 | **Escalation Procedures**  *Procedures to document and obtain approval for unapproved data uses.*  *Generally, contact concerned individual(s) first unless otherwise defined and justified.*  *If data includes “electronic communications,” procedure must meet Electronic Communications Policy (ECP) requirements.*  *Note: The ECP does allow for access without prior authorization in “Emergency Circumstances,” but authorization must then be sought without delay.* |  |
| 7 | **Disclosure to Partners Outside of Monitoring Unit**  *List entities outside the monitoring unit that will have access to the data, e.g., software vendors, campus partners* |  |
| 8 | **Privacy Impact**  *Describe the privacy impact and potential privacy harms to those being monitored due to collection and retention of data. Consider:*  ***a) Use Cases*** *listed above*  ***b) Required Legal Disclosure:***  *e.g., valid subpoena, court order, public records request, or national security letter*  ***c) Internal Abuse*** *of the data within the monitoring unit*  ***d) Accidental or Unauthorized Disclosure****, e.g., data breach* |  |
| 9 | **Privacy Mitigations**  *Procedures, limitations, controls, etc., that will be taken to reduce privacy impacts. Include consideration of the above scenarios and principles of:*  ***a) Least Perusal:***  *Least invasive access to data necessary for meeting stated objectives: automated analysis over manual perusal when possible*  ***b) Least Disclosure:***  *Planned disclosures minimized to the least amount necessary for meeting stated objectives*  ***c) Minimal Retention:***  *Retained only as long as needed to meet stated objectives*  ***d) 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* |  |
| 10 | **Transparency Notice**  *(Planned) location and text of general information about Monitoring Practice published to users* |  |
| 11 | **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.* |  |
| 12 | **Compliance**  *a) Procedures for ensuring ongoing compliance*  *b) Recourse/Grievance procedures* |  |