UMASS BOSTON

**HUMAN RESOURCES**
UNIVERSITY OF MASSACHUSETTS BOSTON

# HR Direct Access Request Form

**Instructions:** New users are required to sign a Computing Awareness and Data Security Compliance Statement and attend training prior to receiving access. After filling out this form, forward to the Department of Human Resources.

□ **ADD** □ **DELETE** □ **CHANGE**

| | | | |
|---|---|---|---|
| Name: | | Position: | |
| Employee ID #: | | Office (Building/Floor/Room): | |
| Department. #: B | | Email: | |
| Dept. Name: | | Phone #: | |
| Status: | □ Employee | □ Student Employee | □ Contingent Worker |
| If access should be temporary, please note start and end dates: | | _____/____/______<br>Start Date | ____/____/______<br>End Date |

## Access Requested

Briefly describe your need to access this data or your HR related job function requiring this access:

**GENERAL ACCESS TO DIRECTORY DATA**

| | |
|---|---|
| □ | Police Officer |
| □ | Telephone Operator |
| □ | Department Staff |

**DEPARTMENTAL RELATED ACCESS**

| | |
|---|---|
| □ | Department Manager |
| □ | Department Timekeeper |
| □ | Time Approver |
| □ | ePAF Initator |
| □ | ePAF Approver |
| □ | Faculty Events Manager |
| □ | Other (please specify): |

**HR Data Access:**
If this user needs access to departmental data in addition to their own, please list those departments (DeptID):

**Time & Labor Approval:**
If this user will be entering Time & Labor for a department, please list those departments (Group ID):

| | |
|---|---|
| **EMPLOYEE SIGNATURE** | Date |

Approved by (Department Head/Chair)

| | |
|---|---|
| **DEPARTMENT HEAD SIGNATURE** | Date |
| **NAME (PLEASE PRINT)** | Position |

Completed requests should be sent to the Data Custodian in Human Resources for approval.

**HUMAN RESOURCES**
UNIVERSITY OF MASSACHUSETTS BOSTON

HR Direct Access Worksheet

**Instructions:** For use by Data Custodian and Security Administrators only.

□ **ADD** □ **DELETE** □ **CHANGE**

| | |
|---|---|
| Name: | Position: |
| Employee ID #: | Office (Building/Floor/Room): |
| Department. #: B | Email: |
| If access should be temporary, please note start and end dates: | _____/____/______ Start Date     ____/____/______ End Date |

## Access Requested

| A / D | HCM ROLES |
|---|---|
| □ / □ | HCMU_TL_TIMEKEEPER |
| □ / □ | HCMU_TL_TIME_APPROVER |
| □ / □ | HCMU_TL_EMPLOYEE |
| □ / □ | HCMU_RT_QUERY_RUN |
| □ / □ | HCMU_PROCESS_MONITOR |
| □ / □ | HCMU_HR_DEPT_MGR_VIEW |
| □ / □ | HCMU_GT_INITIATOR |
| □ / □ | HCMU_GT_GRANTS |
| □ / □ | HCMU_GT_DEPT_APRV |
| □ / □ | HCMU_GT_DEAN_DIR |
| □ / □ | HCMU_CC_FERPA_VIEW_ONLY |
| □ / □ | HCMU_CA_FIN_AID_RPTS |
| □ / □ | HCMU_ACCESS_TO_ALL_POI |
| □ / □ | HCMA_RP_RUN_UMPAY711 |
| □ / □ | Other (please specify): |

| A / D | SUMMIT ROLES |
|---|---|
| □ / □ | SUMMIT_COMMON_UMBOS |
| □ / □ | SUMMIT_HCM_DEPT_ADMIN |
| □ / □ | SUMMIT_HCM_TIME_MANAGEMENT |
| □ / □ | SUMMIT_HCM_TIME_APPROVER |
| □ / □ | SUMMIT_HCM_PAYROLL_ADMIN |
| □ / □ | SUMMIT_HCM_LEAD_BOS |
| □ / □ | SUMMIT_HCM_IMMIGRATION_MGT |

**HR Data Access:**
If this user needs access to departmental data in addition to their own, please list those departments (DeptID):

**Time & Labor Approval:**
If this user will be entering Time & Labor for a department, please list those departments (Group ID):

**Approved by (Data Custodian)**

| | |
|---|---|
| **DATA CUSTODIAN SIGNATURE** | Date |
| **NAME (PLEASE PRINT)** | |

Completed worksheets should be sent to the Security Administrators in IT Services for processing.
Data Custodian and HR Training Lead will be notified when processing is completed.

UMASS BOSTON

**UNIVERSITY OF MASSACHUSETTS BOSTON**
INFORMATION TECHNOLOGY SERVICES DIVISION

University of Massachusetts Computer Awareness and Data Security Compliance Statement

## Computer and System Usage

As an employee of the University of Massachusetts (the University), I understand that the unauthorized use or misuse of University computer facilities, computer applications, computer systems, and/or electronic communications systems (including e-mail) constitutes an infraction of the University's data and computing policies/guidelines.

I will not share or release any logon, operator id or password used to access University data, computer systems, or electronic communications systems. I will keep my password(s) confidential, will change my password as required by the computer system and will select a password that is difficult to guess. I will not store access passwords in batch files, in automatic login scripts, in terminal function keys, in computers without access control or in other locations where another person might discover them.

I will not intentionally write, produce, generate, copy, propagate or attempt to introduce a computer virus, worm, Trojan horse, etc. into any University computer system or any computers linked to the University computer system.

I further acknowledge that I will not use University data or computing systems (e.g. software, hardware, network components, etc.) in any illegal, unethical or unauthorized commercial activities.

## Data Confidentiality

I recognize my individual responsibility for safeguarding the integrity, accuracy and confidentiality of data that I access as dictated by state and federal law, and University policies and procedures.

I will not improperly release any information obtained as a result of my authorized access.

I will properly create, access, use and dispose of University data based on the data's classification.

## Software Usage

I will not knowingly violate the terms of University license agreements for software. I recognize that the University licenses the use of commercial software and does not own this software or its related documentation or instructional material, and except to the extent authorized by the software developer, does not have the right to copy computer software. I will use documentation only as allowed by the vendor and federal Copyright law.

I will not use personally owned software in University computers unless I have a proper license for the software and the license authorizes such use. I will only use such personally owned software in University computers after I have first obtained clearance from appropriate systems personnel as to its compatibility with University computers and systems.

I will not illegally distribute copyrighted software within or outside the University through any mechanism, electronic or otherwise. I will not use my e-mail access to unlawfully solicit or exchange copies of copyrighted software.

*(1) As directed by Board of Trustees' Policy Statements on Electronic Data Security, Electronic Mail and Computer Policy Development (Doc. T97-010, adopted February 5, 1997), and Policy Statement on Record Management, Retention and Disposition (Doc. T99-061 adopted August 4, 1999). Full text of these Policies and related Guidelines and all University Data and Computing Guidelines can be found at: https://www.umassp.edu/bot/policies*

UMASS BOSTON

## Electronic Communications

I will use e-mail and any other electronic communications tool in a responsible manner consistent with other business communications (e.g., phone, correspondence). I will safeguard the integrity and confidentiality of University electronic mail; only use mail IDs assigned to me and will remove mail from my mailbox consistent with University, campus, departmental or electronic mail administrator message retention procedures.

I will not "rebroadcast"/send to a third party information obtained from another individual that the individual reasonably expects to be confidential, except as required by my job responsibilities, University policies and procedures, and applicable law.

I will not post materials that violate existing laws or University policies/codes of conduct. For example, materials that are of a fraudulent, defamatory, harassing, or threatening nature. I will not unnecessarily or inappropriately use computer resources by sending chain e-mails, spamming, mail bombing, generating unnecessary excessive print, etc.

## My Responsibilities

I have agreed and will attend a workshop that includes information regarding my computer security and data confidentiality responsibilities as an employee of the University. I understand these responsibilities both as an authorized user and an employee.

I recognize my overall responsibility to exercise the degree of care required to maintain control of University computing systems and resources (e.g., data, software, hardware, network components, etc.) and agree to abide by established University policies/guidelines and Campus procedures. I acknowledge that failure to comply with University data and computing related policies/guidelines/procedures might result in: the loss or restriction of my computer access; reprimand; suspension; dismissal, or other disciplinary or legal action.

*Print Name*

*Signature* *Date*

*(1) As directed by Board of Trustees' Policy Statements on Electronic Data Security, Electronic Mail and Computer Policy Development (Doc. T97-010, adopted February 5, 1997), and Policy Statement on Record Management, Retention and Disposition (Doc. T99-061 adopted August 4, 1999). Full text of these Policies and related Guidelines and all University Data and Computing Guidelines can be found at: https://www.umassp.edu/bot/policies*