University of Hawai‘i
General Confidentiality Notice (revised 7/31/20)

I understand that as part of my duties and responsibilities as a University of Hawai‘i employee or affiliate, I may have access to Protected Data which are data subject to security and privacy considerations (and are classified as Restricted, Sensitive, and Regulated in Executive Policy 2.214). Activities may involve the collecting, managing, sharing, exchanging, using, and/or releasing such data and often may involve personally identifiable information (PII) where a data element, or a combination of data elements, when considered together, would identify an individual. Such data may include, but are not limited to:

- Student and employee contact information (home and mailing address, phone number, email address)
- Demographic data (date of birth, age, ethnicity, etc.)
- Admission and academic records
- Job applicant records (names, transcripts, etc.)
- Employment and payroll records
- Social Security Number
- Credit card or credit-related information
- Bank account information
- Health data
- Financial aid (FAFSA) data

I understand that the confidentiality of Protected Data is protected by a number of federal and state laws and University of Hawai‘i policies, including Federal Family Educational Rights and Privacy Act (FERPA); the Higher Education Act (HEA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Hawai‘i Revised Statute (HRS) Chapters 487N and 92F, Payment Card Industry Data Security Standard (PCI-DSS), and others.

I understand that it is my responsibility to respect and protect the confidentiality of this information and that the Protected Data entrusted to me will be used only for the purpose of fulfilling the requirements of my assigned task/project or used only within the authorized scope of my research study. I understand that seeking access to Protected Data beyond the scope of fulfilling my responsibilities is prohibited.

I further understand that disclosing, using or altering any such information without proper authorization is prohibited. If I have any questions regarding access, use, or disclosure of such information, it is my responsibility to consult with the appropriate University data steward or UH liaison prior to taking any action. Additionally, it is my responsibility to restrict access to the data. This includes keeping my server or personal computer log in information confidential. I shall not allow others to use my active sessions other than to resolve specific problems. It is my responsibility as a UH employee to notify my supervisor and the UH Information Security Officer in Information Technology Services (or as a non-UH employee, to notify my UH liaison) immediately should the Protected Data under my care be compromised or publicly exposed in any way.

I understand that electronic transactions on UH information systems may be automatically logged and that the logs of my actions may be routinely reviewed as part of the University’s information security assurance program. I understand that if I store any Protected Data on any personal computer or server, it is my responsibility to ensure that the hardware/software are secured and managed in accordance with applicable University policies and procedures. I have read and understand my responsibilities under UH Executive Policy 2.210 “Use and Management of Information Technology Resources” (http://www.hawaii.edu/policy/ep2.210) and UH Executive Policy 2.214 “Institutional Data Classification Categories and Information Security Guidelines” (http://www.hawaii.edu/policy/ep2.214).

I understand that failure to abide by this notice may result in disciplinary action in accordance with University policies and procedures, state and federal laws, and applicable collective bargaining agreement up to and including dismissal.