# OLD DOMINION UNIVERSITY
## University Policy

Policy #3501
INFORMATION TECHNOLOGY ACCESS CONTROL POLICY

Responsible Oversight Executive: Vice President for Administration and Finance
Date of Current Revision or Creation: May 10, 2022

and related information, equipment, goods, and services.

User- I

business through contractual arrangements, including, but not limited to, all employees, students, volunteers, and visitors to the institution. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. Students include all persons admitted to the University who have not completed a program of study for which they were enrolled; student status continues whether or not the University's programs are in session. Visitors include vendors and their employees, parents of students, volunteers, guests, uninvited guests, and all other persons located on property, owned, leased, or otherwise controlled by the University

E. POLICY STATEMENT

The University will provide all employees and other users with the information they need in order to carry out their responsibilities in as effective and efficient manner as possible. Access to data will be limited to authorized individuals whose job responsibilities require it, as determined by an approval process, and to those authorized to have access by Federal or State laws or in accordance with University policies and standards. The process for requesting, granting, administering, and terminating accounts on IT systems, including accounts used by vendors and third parties, is provided in Information Technology Standard 04.2 Account Management Standard.

Access is given through the establishment of a unique account in accordance with account request procedures. Exceptions to the establishment of unique accounts may include stand-alone personal computers, public access computers or related resources, and student labs where individual student accounts are not required.

All users of IT systems are responsible for reading and complying with university information technology requirements, reporting breaches of IT security, actual or suspected, to University management and/or the Information Security Officer, taking reasonable and prudent steps to protect the security of IT systems and data to which they have access, and complying with any Federal, State, or local statutes and University policies and standards as might apply to these resources. Every user must maintain the confidentiality of information assets even if technical security mechanisms fail or are absent.

Old Dominion University reserves the right to revoke any user's access privileges at any time for violations of policy, standards and/or conduct that disrupts the normal operation of information technology resources.

F.

POLICY HISTORY
**********
Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Rusty Waterfield — May 5, 2022
Responsible Officer — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna W. Meeks — April 19, 2022
Chair, Policy Review Committee (PRC) — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Chad A. Reed — May 5, 2022
Responsible Oversight Executive — Date

University Counsel Approval to Proceed: