Richard Bland College
Information Technology Services
11301 Johnson Road
Petersburg, Virginia 23805

Richard Bland College Information Technology Resources

Student Acceptable Use Policy rev: 4

Approved by: Richard Bland College Information Security Officer

Richard Bland College
Student Acceptable Use Policy (SAUP)

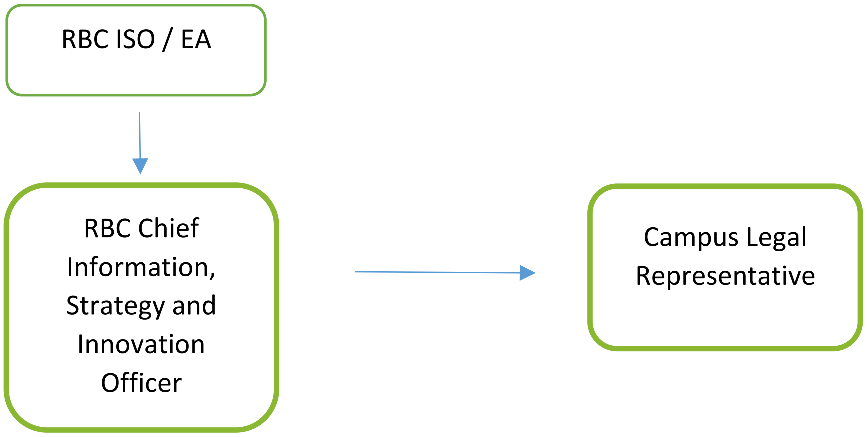
Version Control

It is the end user's responsibility to ensure they are accessing/utilizing the latest version of the Technology Resources Information Security Standard. Questions should be directed to the Richard Bland College Information Security Officer / Enterprise Architect.

History of Security Standard revisions

Version	Date	Purpose of Revision
Original	11/20/2015	Base document
Revision 1	1/20/2016	Revision to align with best practices
Revision 2	5/20/2016	Revision in alignment with network upgrade
Revision 3	2/15/2017	Revision to align with current Technology Resources environment
Revision 4	2/27/2017	Revision to finalize scope and purpose. Included statement of privacy and rights and responsibilities

Review Process:


RBC ISO / EA
RBC Chief Information, Strategy and Innovation Officer
Campus Legal Representative

Contents

Purpose

The computing resources at Richard Bland College of William & Mary (RBC) support the educational, instructional, and administrative activities of the College and the use of these resources is a privilege that is extended to members of the RBC community. Users of these services and facilities have access to valuable College resources, to sensitive data, and to internal and external networks. Consequently, it is important to behave in a responsible, ethical, and legal manner.

In general, acceptable use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements. If an individual is found to be in violation of the Acceptable Use Policy, the College will take disciplinary action, up to and including suspension from the College or termination of employment. Individuals are also subject to federal, state and local laws governing interactions that occur on RBC information technology resources.

This document establishes specific requirements for the use of all computing and network resources at Richard Bland College of William & Mary.

Scope

The RBC Acceptable Use policy applies equally to all individuals utilizing RBC information technology resources (e.g., employees, faculty, students, alumni, agents, consultants, contractors, volunteers, vendors, temps, etc.).

Information technology resources include all college owned, licensed, or managed hardware and software, and use of the college network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

An attempt to violate policy will be considered the same as an actual policy violation. An "attempt" is any act beyond mere preparation carried out with the intent to engage in conduct that is in violation of policies.

Rights and Responsibilities

As members of the College community, users are provided with the use of scholarly and/or work-related tools, including access to the Library, to certain computer systems, servers, software and databases, to the campus telephone and voice mail systems, and to the Internet. There is a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy (which may vary depending on whether the user is a College employee or a matriculated student), and of protection from abuse and intrusion by others sharing these resources.

In turn, users are responsible for knowing the regulations and policies of the College that apply to appropriate use of the College’s technologies and resources. Users are responsible for exercising good judgment in the use of the College's technological and information resources. Just because an action is technically possible does not mean that it is appropriate to perform that action. Users are representatives of the RBC community, and are expected to respect the College’s good name in electronic dealings with those outside the College.

Privacy

All users of state networks and systems should keep in mind that all usage of information technology resources can be recorded and is the property of Richard Bland College of William & Mary. Such information is subject to the Freedom of Information Act and the laws applicable to state records retention. Employees have no right to privacy with regard to use of state-owned resources. RBC management has the ability and right to view users’ usage patterns and take action to assure that college resources are devoted to authorized activities.

Electronic files created, sent, received, or stored on RBC information technology resources that are owned, leased, administered, or otherwise under the custody and control of RBC are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Virginia Administrative Code.

Acceptable Use

The RBC network exists to support education, and administrative activities by providing access to computing resources and the opportunity for collaborative work. Primary use of the RBC network must be consistent with this purpose and the educational mission of the College.

Access to the RBC network from any device must adhere to all the same policies that apply to use from within RBC facilities.

1. Users may use only RBC information technology resources for which they are authorized.
2. Users are individually responsible for appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware, and are accountable to the College for all use of such resources. Authorized users of Richard Bland College resources may not enable unauthorized users to access the network. The university is bound by its contractual and license agreements respecting certain third-party resources; users must comply with all such agreements when using RBC information technology resources.

3. Users should secure resources against unauthorized use or access to include RBC accounts, passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
4. Users must report shareware or freeware that is installed on RBC-owned equipment unless it is on the approved software list. When software is installed, it must be reported to the STAC via email (stac@rbc.edu).
5. Users must not attempt to access RBC information technology resources without appropriate authorization by the system owner or administrator.

Restrictions

All individuals are accountable for their actions relating to RBC information technology resources. Direct violations include the following::

1. Interfering or altering the integrity of RBC information technology resources by:
   a. Impersonating other individuals in communication;
   b. Attempting to capture or crack passwords or encryption;
   c. Unauthorized access, destruction or alteration of data or programs belonging to other users;
   d. Excessive use for personal purposes, meaning use that exceeds incidental use as determined by supervisor;
   e. Use for illegal purposes, including but not necessarily limited to violation of federal or state criminal laws;
2. Allowing family members or other non-authorized persons to access RBC information technology resources.
3. Transmitting unsolicited messages and communication to and/or from Richard Bland College email containing obscenity, harassment, bullying, or threats;
4. Utilizing College systems and resources in any manner inconsistent with the intended purpose, including but not limited to commercial, business, illegal, or private gain.
5. Making unauthorized copies of licensed software and/or copyrighted materials, including media and entertainment resources;
6. Violating legal mandates such as the Digital Millennium Copyright Act (DMCA);
7. Utilizing peer to peer file sharing applications;
8. Installing pirated or illegally obtained software, utilities, media, and applications;

9. Knowingly engaging in any activity harmful to the computers, systems, and resources such as creating or propagating malware, overloading networks with excessive data, instituting or promulgating chain letters, or instigating unauthorized mass postings of any type
10. Deliberately circumventing or subverting security measures.
11. Interfering with the use of RBC resources which inhibit or interfere with the use of resources by other authorized users (for example, applications which use a disproportionate amount of bandwidth for extended periods)