Policy-Acceptable Use of Electronic Resources

The company makes computing resources (including, but not limited to, computer facilities and services, computers, networks, electronic mail, electronic information and data, and video and voice services) available to staff, interns, and the general public to support the enterprise requirements of the company.

# Scope

When demand for computing resources may exceed available capacity, priorities for their use will be established and enforced. Authorized staff may set and alter priorities for exclusively local computing/networking resources. The priorities for use of Link3’s -wide computing resources are:

* ***Highest Business Impact (HBI)****:* Uses that directly support the research and service missions of the company.
* ***Medium Business Impact (MBI)****:* Other uses that indirectly benefit the research and service missions of the Link3’s, as well as and including reasonable and limited personal communications.
* ***Lowest Business Impact (LBI)****:* Recreation, including game playing.

*Forbidden:* All activities in violation of the General Standards or prohibited in the *Specific Rules* interpreting this policy.

# Content of communications

1. Except as provided by applicable government laws, regulations or other Link3’s policies, the content of electronic communications is not by itself a basis for disciplinary action.
2. Unlawful communications, including threats of violence, obscenity, pornography, and harassing communications (as defined by government labor law), are prohibited.
3. The use of computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized under applicable Link3 policies), fundraising or advertising on behalf of any organization, or the reselling of Link3’s computer resources to individuals or organizations, and the unauthorized use of the Link3's name, are prohibited. The CISO for Information Systems (or designee/TBA) may specify rules and specific forums where limited use of Link3 resources for non-recurring exchange and sale of personal items is permitted.

# Access to computer resources

The following activities and behaviors are prohibited:

1. The use of restricted-access Link3’s computer resources or electronic information without or beyond one's level of authorization (access by penetration);
2. The interception or attempted interception of communications by parties not explicitly intended to receive them without approval of an authorized/management personnel;
3. Making organizational computing resources available to individuals not affiliated with the company; without approval of an authorized Link3’s staff;
4. Making available any materials the possession or distribution of which is illegal;
5. The unauthorized copying or use of licensed computer software by using any keygrabber;
6. Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under Link3's policies regarding privacy or the confidentiality of personnel, archival, or other records, or as defined by the cognizant Data keeper.
7. Intentionally compromising the privacy or security of company owned electronic information; and
8. Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction).

# Operational integrity

The following activities and behaviors and patters are prohibited:

1. Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of electronic chain mail, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts or audiences;
2. Failure to comply with requests from appropriate official staff to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy;
3. Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access;
4. Altering or attempting to alter files or systems without authorization;
5. Unauthorized scanning of networks for security vulnerabilities;
6. Unauthorized access to staff’s computer without prior consent from the staff;
7. Unauthorized recording of IP Phone conversation;
8. Unauthorized usage of video footage usage, recorded by floor cams;
9. Unauthorized data capture to/from any company owned devices or staff computers or BYO devices;
10. Attempting to alter any computing or networking components configuration (including, but not limited to, bridges, routers, and hubs) without authorization or beyond one's level of authorization;
11. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services;
12. Intentionally damaging or destroying the integrity of electronic information;
13. Intentionally disrupting the use of electronic networks or information systems;
14. Intentionally snooping on someone’s (company staff) data traffic, without written authorization;
15. Intentionally wasting/shredding or electronic resources; and
16. Negligence leading to the damage of electronic information, computing/networking equipment and resources.

# Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# Distribution

This policy is to be distributed to all Staff members with access to Company’s Information Resources.