

Section:	FB-4 Finance and Business Services	Approval Date:	7/28/2017
Policy:	FB-4.7 Information Technology	Latest Revision:	6/4/2021

FB-4.7 Information Technology

4.7.1 Purpose

The following policies are intended to guide the Association in the responsibilities, needs, application, and use of all Association technology.

4.7.1.1 Hardware and Software Purchases

Any purchase of computer hardware or software is subject to the same limitation as other Association purchases (i.e., appropriate budget authorizations, etc.). All purchases must have the approval of the requesting department manager and the Senior Director of Operations and Member Engagement after consultation with the Chief Technology Officer based on compatibility and functionality with existing systems and future plans (i.e., upgrades, etc.). Software and hardware are to be installed and configured by the Information Technology Group.

4.7.1.2 Authorized Software

Only software in which the Association has obtained a license agreement to operate and verified its compatibility with existing software/hardware and operating system(s) will be placed on any Association personal computer. As new software is approved and obtained, it will be added to a catalog of approved software maintained by the Information Technology Group together with licensing agreements. Unauthorized and personally owned software may not be installed on any Association computer equipment.

4.7.1.3 Backup

The Information Technology Group will regularly and systematically back up all data and store it in the cloud.

4.7.1.4 Service

The responsibility for service and maintenance of personal computers, devices, and all technology-related matters lies with the Information Technology Group. The Information Technology Group has a formal process to resolve technology related issues/requests (Helpdesk).

4.7.2 Security

Personal computers are the gateway to the Local Area Network which contains both public and confidential information. Access is controlled by the use of a User ID and password. The Information Technology Group will work with new employees to develop User IDs and initial passwords upon start of employment. Staff will select and maintain their passwords until departure of employment with the Association. New staff shall receive orientation on security, its importance, and relevance.

User IDs and passwords are intended to keep confidential materials secured to those individuals needing access and therefore protected from unauthorized entry. Several core systems utilized by the Association are hosted in the cloud. Access to those systems is granted via a single User ID and password. The Information Technology Group has a formal process that requires users to reset their passwords periodically.

4.7.3 New Staff Training and Orientation

New staff will receive training and orientation in the use of the following Association tools:

- Security
- Local Area Network sign-on and sign-off process
- Windows applications used by the Association
- Telephone usage and features
- Customer Relationship Management System (CRM)
- Microsoft Office Suite (Word, Excel, PowerPoint, etc.)
- Electronic Time Sheet System
- Electronic Employee Expense Reporting

References:

Previous Board Policy H. 1-2. See ACWA Personnel Manual, Policy 4.5, Technology Resources.

See Administrative Procedure: *To be determined.*

Revision History:

Revision Date	Description of Changes	Requested By
7/28/2017	Initial Release	ACWA Staff and Governance Workgroup
6/4/2021	Revised Policy 4.7.1.1 Hardware and Software Purchases to delete reference to the Director of Finance and Business Services and replace with updated language.	ACWA Staff based on organizational changes approved by the Executive Committee and Board of Directors, effective January 2021.