**The Putnam County Community Foundation**

**Possible Information Technology Security Practices**

**Page 1 of 2**

# Change IP address periodically

# Password protection

# Require complex passwords – 11 digits min, upper case, lower case, numbers, symbols, no words, not personally identifiable;

# System forced password change every 90 days;

# Passwords protected (kept in secure location).

# Network Administration security

# Require complex passwords – 11 digits min, upper case, lower case, numbers, symbols, no words, not personally identifiable;

# System forced password change every 90 days;

# Passwords protected (kept in secure location).

# Set up administration passwords so that network administrator can lock out a user;

* 1. Set up administration password so that designated employee can lock out network administrator.

# Wi-Fi wireless security -- Evaluate security of network vs. security of Wi-Fi users in decision to run Wi-Fi through firewall.

# Website Security – Implement regular virus scans

# Server / Network Protections

# Physical Security

* + 1. Temperature control
		2. Smoke detectors checked yearly; batteries replaced
		3. Fire Extinguishers checked yearly
		4. Protection from power surges via USP battery backups for servers and workstation.
		5. Set up to eliminate cabling stress.
		6. A physically secured space with controlled access – locked cage for server
		7. Electrostatic discharge protection
	1. Firewall and firewall maintenance plan
	2. Endpoint security protections: i.e. Barracuda, Kaspersky, Malwarebytes, Norton, etc. Constant scanning. Provide Smart reports -- Immediate notification of errors and findings

## MAC address control of users enabled for all devices

* 1. Consider cost benefit of having duplicate spare parts for critical devices, i.e. firewall, switch, router.
	2. Set up controlled access / Selective access rules: PCs, Folders, Files, Drives, Time of Day, etc.
	3. Install software updates in a timely manner -- automatically if possible.

# Copiers / Printers / Scanners

* + 1. Change IP numbers periodically
		2. Schedule regular virus scan;
		3. Maintain/install current firmware

# Work stations

* 1. Forced session log outs after 15 minutes.
	2. Forced monitors switch to screen savers after 15 minutes.
	3. Disable USB ports at the workstation level
	4. Regularly install current firmware.

## Liability

* 1. Cyber liability insurance
	2. No bank account numbers, social security numbers or credit card numbers maintained electronically.
1. **Data security**
	1. All work saved on server; nothing saved exclusively on workstations.
	2. Data backed up daily from servers onto hard drives – 30 days data stored on hard drive. Two hard drives taken off site daily and rotated.
	3. Back Up hard drives protected from damp, heat, cold, magnets, theft.
	4. Daily email notification of back up success /failure to multiple persons.
	5. Twice annual check of hard drive data to be sure accessible and complete.
	6. System of semi-annual or annual back up storage in addition to daily/30 days.

# VPN Security

# Secure operating system utilized -- all data is encrypted.

# Ensure off site devices being utilized are protected and virus free.

# New hire and annual security training

* 1. Roles and responsibilities.
	2. Acceptable Use of IT equipment;
	3. Acceptable use of employee devices;
	4. Acceptable use of USB ports.
	5. Vendor access/verification
	6. Pfishing/Internet use
	7. Authentication procedures

# Board education and oversight

# Annual IT security audit and report

1. **Recovery Plan**
	1. Back up server
	2. Paper processes in event of no IT capabilities