CONTROL 4.1 · 4.2 · GOVERN

# New Device & Network Setup Checklist

Run through this whenever you set up a new computer, tablet, or router. Keep a copy with your business documents. Be sure to include all devices in the spreadsheet you got from our site under tab “Devices (1.1)”.

- ☐ Change the default password on the new device or router
- ☐ Turn on automatic updates
- ☐ Turn on the built-in firewall
- ☐ Keep business devices on your main network; put visitors on a separate guest Wi-Fi
- ☐ Write down the settings you used, and where you saved them
- ☐ If you use an IT provider (MSP), ask them to document their standard setup

> 🌸 **FLO’S FLOWER SHOP**
> Flo asked the nephew who set up her router to write down exactly what he changed. She keeps it with her other business papers and follows the same steps for every new tablet.

CONTROL 6.1 · 6.2 · GOVERN

# Giving and Removing Access

Use this when someone joins or leaves. The “leaving” side is the one most businesses forget — and it’s how a lot of attacks get in.

### When someone JOINS

- ☐ Decide what they actually need — give the least access required
- ☐ Create or grant only those accounts
- ☐ Turn on MFA (multi-factor authentication) for their logins
- ☐ Add them to your Accounts list

### When someone LEAVES — the same day

- ☐ Disable their logins
- ☐ Change any shared passwords they knew
- ☐ Remove them from email, POS, accounting, and any other systems
- ☐ Update your Accounts list

> 🌸 **FLO’S FLOWER SHOP**
> A seasonal helper gets the POS only — not email or accounting. Flo’s five-minute offboarding checklist gets done before they walk out the door.

CONTROL 11.1 · GOVERN

# Data Recovery Plan

If ransomware hits, this page is the difference between a bad week and a closed business. Fill it in now — and keep it somewhere you can reach without your computer.

| | |
|---|---|
| **What's backed up** | |
| **Where the backup lives** | *(best: two places — e.g., cloud + an offsite drive)* |
| **How often it runs** | |
| **Date we last TESTED a restore** | |
| **Who to call first (IT provider)** | |
| **Cyber insurance claims line** | |

### Steps to restore (write them while things are calm)

| | |
|---|---|
| **1.** | |
| **2.** | |
| **3.** | |

> 🌸 **FLO'S FLOWER SHOP**
> If you've never actually restored from a backup, you don't really have a backup. Test it once a year and write the date above.

CONTROL 14.1 · GOVERN

# Security Training: Basics + Log

Most ransomware starts with a fake email. A 20–30 minute session once a year is one of the best investments you can make.

### The basics to cover (your handout)

- Most attacks start with a fake email or text.
- The rule: if a message asks you to click a link or open a file you weren't expecting, stop — call the sender on a number you already trust.
- When in doubt, don't click. Ask first.

### Training log

| Date | Who attended | What we covered | Notes |
|---|---|---|---|
| Jan 2026 | Flo + 2 staff | Phishing, the call-back rule | Done |
| *( )* | | | |
| *( )* | | | |

> 🌸 **FLO'S FLOWER SHOP**
> Every January, Flo spends 20 minutes with her team on the basics and writes the date down. That's it — that's the program.

CONTROL 17.3 · GOVERN

# If We Get Hit: Break-Glass Card

Print this. Keep a physical copy where staff can find it — in an attack, you may not be able to get to a computer.

## First three steps

1. Disconnect affected machines from the internet (unplug the cable or turn off Wi-Fi).
2. Call our IT provider (number below).
3. Report the attack to the FBI at ic3.gov.

**Don't decide whether to pay on your own.** The FBI advises against paying — your IT provider, your insurer, and the FBI can help you weigh it.

## Key numbers

| | |
|---|---|
| **IT provider** | |
| **Cyber insurance claims** | |
| **CISA (24/7)** | **1-844-729-2472** |

*If customer data was exposed, your state may require you to notify customers.*

> 🌸 **FLO'S FLOWER SHOP**
> Flo taped a laminated card inside the top drawer of her desk. The card has three phone numbers, three steps, and her staff know where it is.