Security Guidelines

Opossum Dynamics Internal Protocol – Security Division

Overview

At Opossum Dynamics, security is not just a suggestion — it's an elaborate set of guidelines loosely enforced across multiple pop-up office locations. These protocols are designed to protect our assets, disrupt attackers, and occasionally confuse everyone involved.

Failure to follow these rules may result in unauthorized building access, data leaks, or the unintentional summoning of legal action.

Physical Security Rules

1. Don’t Let Strangers In.
If someone you don’t recognize tailgates you through a door, assume it’s a test. Slam it shut. If they yell “I work here!”, that’s not a password.

2. Badge Usage Is Mandatory.
Wear your badge at all times. Do not lend your badge to Greg. He already has one (we think).

3. Lock All Entry Points.
Doors. Windows. Trapdoors. Secret bookcases. You are responsible for your immediate area’s structural integrity.

4. Know the Safe Word.
Each department has a rotating safe word. If someone enters your workspace and doesn't know it, detain them using the de-escalation technique outlined in the Training Binder (Vol. IV).

5. Desk Security.
If you leave your workspace unattended for more than 6 seconds, lock your device and cover all confidential information with an Official Opossum Dynamics Security Blanket™.

Digital Security Rules

1. Change Your Password When Threatened.
This includes: phishing emails, suspicious DMs, Greg looking at you too long, or receiving a fruit basket from an unknown source.

2. Never Share Passwords, Even With Yourself.
You in the morning is not the same as you at 3 AM during a Red Team exercise. Keep secrets.

3. Use Two-Factor Authentication.
Your second factor must involve either biometric data or direct eye contact with the IT raccoon (see appendix D).

4. Report Suspicious Activity.
Examples include:

- Someone asking what your password is
- Someone offering to help with “tech stuff”
- Your mouse moving on its own (unless you authorized remote access or the ghost is back)

Social Engineering Awareness

Do not accept candy, coffee, or compliments from unknown individuals.
These are standard social engineering tactics. Also, flattery is not permitted without clearance.

Security Drills May Not Be Announced.
You may be “tested” at any time by another employee. These tests may involve break-ins, phishing, fake executives, or Greg in disguise.

Penalties

Violations of security policies will result in disciplinary actions ranging from stern emails to being volunteered as a penetration test target.