Information security policy: what every employee must do

Northmere Logistics · Policy IS-01, staff summary · Version 5 · Applies to all employees and contractors · Sample policy written for the DocReel demo

Why this policy exists

We hold customers' addresses, delivery records and payment details. Most security incidents don't start with a clever attack. They start with one person clicking a link, reusing a password or leaving a laptop unlocked. This summary covers the five rules that apply to everyone, and what to do when something goes wrong.

The five rules

1. **Use a strong, unique password and two-step sign-in.** Your work password must be at least 14 characters and used nowhere else. Use the company password manager. Two-step sign-in is required on every work account.
2. **Stop and check before you click.** Be suspicious of any message that is urgent, unexpected, or asks for a password, a payment or a gift card. Check the sender's address, not just the name.
3. **Lock it when you leave it.** Lock your screen every time you step away. Never leave a laptop or phone in a vehicle overnight.
4. **Keep customer data in approved systems.** Don't send customer data to personal email, save it to personal cloud storage, or paste it into tools the company has not approved.
5. **Report it fast.** If something looks wrong, report it within one hour, even if you are not sure and even if it was your mistake.

How to spot a phishing message

Warning sign	Example
Pressure to act now	“Your account will be closed in 30 minutes.”
A sender address that is slightly wrong	accounts@northrnere-logistics.example
A request to skip the normal process	“Pay this invoice today, I'm in a meeting and can't talk.”
A link that goes somewhere unexpected	Hover over it: the address doesn't match the company named.

> **If you are unsure,** don't reply and don't click. Use the “Report phishing” button in your email, or forward it to security@northmere.example.

What to do if something goes wrong

1. **You clicked a link or entered your password:** change your password straight away, then call the IT security line on ext. 911.
2. **You lost a laptop, phone or ID badge:** call the IT security line at once, at any hour. The device can be locked and wiped remotely.
3. **You sent customer data to the wrong person:** don't try to fix it yourself. Report it. We may have to tell the customer and the regulator within 72 hours, so every hour counts.

> **You will not be punished for reporting a mistake.** Hiding one is a disciplinary matter. An incident reported in the first hour is usually contained; one found a week later rarely is.

Working away from the office

- Use the company VPN on any network that isn't ours, including home and hotel Wi-Fi.
- Don't work on customer data where your screen can be seen, such as on a train.
- Work only on company devices. Personal laptops and tablets are not allowed for customer data.

Your responsibilities

Who	What they must do
Every employee	Follow the five rules and complete this training once a year.
Managers	Make sure new starters complete it in their first week, and remove access on a leaver's last day.
IT security	Answer every report within one hour and run a phishing test each quarter.

Breaking this policy on purpose, or repeatedly, can lead to disciplinary action. The full policy, IS-01, is on the intranet under Policies.

Northmere Logistics is a made-up company. This sample policy was written for docreel.app to show how a compliance policy becomes a training video. It is not legal or security advice.