Data Security: The 12 HR Policies You Need to Stop Employee Data Breaches



The Stakes

In this digital age, safeguarding customers' private information from hackers, identity thieves and other cyber threats isn't just a legal obligation; it's a business imperative. A single data breach can have disastrous results including not only liability and devastating negative press but loss of any company's most important business asset, the trust of its customers. Yet, with so much on the line, data breaches keep happening even at large and sophisticated companies that invest billions in data security. Why?

The Problem

Many data breaches can be traced back to employees. Whether deliberate or inadvertent, the acts or omissions of even a single employee can undermine even the most elaborate data security system.

The 12 Policies You Need to Solve the Problem

While technology is part of the solution, you also need to have the right HR policies to keep your precious customer data secure and prevent data breaches. Here's a look at the 12 policies you need which can be separate or combined with other data security and privacy policies. You can find Model versions of most of these policies on HR Insider by clicking on the listed link.

1. Computer Use Policy

Acceptable use (aka "computer use") policies" set out rules for proper use of company computer and digital resources. Make sure your own acceptable use policy specifies both acceptable and unacceptable uses (Click here for a Checklist of Unacceptable Uses to Ban) of fixed, laptop and mobile computing devices and network resources.

2. Email Use Policy

Employee email mishaps are a leading cause of data breaches. So you need a policy clearly explaining the proper and improper use of your organization's email systems,

including with regard to:

- Information emails and attachments can contain;
- Replying and forwarding of emails and attachments, e.g., banning automatic forwarding of emails containing protected data;
- Measures to keep emails and attachments secure;
- Retention of emails containing protected data.

3. Social Media & Blogging Policy

You also need a policy making it clear to employees that blogging and use of social media is subject to your organization's data security restrictions even when it occurs within their own home after work, including but not limited to policies:

- Banning disclosure of confidential information;
- Requiring employees to behave in a professional manner and refrain from conduct that may harm the reputation, image or goodwill of the organization, employees or clients;
- Banning discrimination and harassment;
- Banning employees from speaking on behalf of the organization without authorization.

Employee Computer, Email & Social Media Use IS Your Business

Be sure to specify in your computer use, email and social media use policy that your organization has the right to monitor their compliance with the respective policy and that employees should have no expectation of privacy in how they use their work computers and organization email systems.

4. Clean Desk Policy

The purpose of this policy is to warn employees against carelessly leaving sensitive data out in the open. Make sure your policy lists what employees must do to secure personal data in their work area when they go home at night or leave their workstation for an extended period, including verifying that:

- Computers are shut down and secured;
- Hardcopy documents are removed and locked in secure files or drawers;
- Drawers and file cabinets are locked and the key isn't left unattended;
- Whiteboards are erased;
- Printers and fax machines are cleared of papers as soon as printing is done.

5. Workstation Security Policy

It takes more than physical barriers and technical safeguards like encryption to achieve workstation security. You also need a policy listing the measures employees must take to keep their workstations secure, such as:

- Allowing only authorized personnel into their workstations;
- Making sure workstations are locked when they're away;
- Logging off and securing their computers before leaving at night;
- Complying with password restrictions;
- Not installing unauthorized software ;
- Not using personal devices or systems to store protected data.

6. Password Creation Policy

Inadequate password protection by employees is a major weak spot in data security systems. The first thing you need to address the problem is a policy requiring employees to create strong passwords and listing guidelines, including:

- Standards passwords must meet, e.g., at least 12 alphanumeric characters in length;
- Things to put in passwords, e.g., upper and lower case letters and characters like *&^%#;
- Things not to put in passwords, e.g., birthdates, names and other personal information.

There should also be a clear process for changing passwords.

7. Password Protection Policy

You should also have a policy requiring employees to keep their passwords secure. and banning common mistakes that compromise password security, such as:

- Writing down their passwords on post-its or note pads and compounding the error by leaving the post-it out in the open or even under the desk or another obvious hiding spot;
- Sharing passwords with others;
- Including passwords in emails or disclosing them on the phone;
- Using the same password for multiple accounts;

8. Digital Signature Policy

If you use digital signatures for electronic correspondence, you need a policy setting out clear ground rules for employees including:

- Types of correspondence for which digital signatures are permitted;
- Who within the organization may use a digital signature to validate their identity;
- Criteria for accepting a digital signature as valid, g., a requirement that signers sign their own names and not simply list their title or position;
- What employees should do if they suspect abuses or infractions.

9. Data Removal Policy

Many data breaches are the result not of hacking or deliberate cyberattack but lost and stolen laptops. So you need a policy restricting employee removal of personal data, including:

- A requirement that removals be authorized;
- A clear process for granting such authorization;
- Limitations on what data can be removed; and
- Mandatory safeguards for protecting removed information.

10. Bring Your Own Device (BYOD) Policy

In this era of mobile computing, you need a BYOD policy addressing:

- Whether employees can bring personal electronic devices to work for work-related uses;

- Which devices are approved for BYOD;
- Which uses are acceptable;
- Restrictions on uses, e.g., banning use of personal devices to download organizational files containing personal or proprietary information; and
- Measures employees must take to keep their devices secure, e.g., use of passwords or encryption.

11. Remote Access Policy

Although allowing employees to connect your organization's network from remote locations is vital to productivity, it can also compromise network security. So you need a remote access policy explaining the requirements for connecting to the network from an external network or host, including:

- Who will have remote access privileges;
- Acceptable and prohibited uses for remote access;
- Required measures remote users must take to ensure the connection is at least as secure as the user's on-site connection; and
- Standards for connecting Bluetooth-enabled devices to the network or company-owned devices.

12. Data Breach Response Policy

While prevention is the paramount objective, organizations also need to be prepared to respond to any data breaches that occur. The key to effective response is finding out about the breach as swiftly as possible. And because employees are usually the first to know, you need a policy requiring employees to notify their supervisors immediately of any breaches they know or suspect have occurred.