Data security policy:

Employee requirements

Using this policy

This example policy outlines behaviors expected of employees when dealing with data and provides a classification of the types of data with which they should be concerned. This should link to your AUP (acceptable use policy), security training and information security policy to provide users with guidance on the required behaviors.

1.0 Purpose must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our customers. The protection of data in scope is a critical business requirement, yet flexibility to access data and work effectively is also critical. It is not anticipated that this technology control can effectively deal with the malicious theft scenario, or that it will reliably detect all data. It's primary objective is user awareness and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, a focus for the policy and a rationale.

2.0 Scope
1. Any employee, contractor or individual with access to systems or data.
2. Definition of data to be protected (you should identify the types of data and give examples so that your users can identify it when they encounter it)
☐ PII
☐ Financial
☐ Restricted/Sensitive
☐ Confidential
☐ IP 3.0 Policy – Employee requirements
1. You need to complete 's security awareness training and agree to uphold the acceptable use policy.
2. If you identify an unknown, un-escorted or otherwise unauthorized individual in you need to immediately notify .
3. Visitors to must be escorted by an authorized employee at all times. If you are responsible for escorting visitors you must restrict them appropriate areas.
4. You are required not to reference the subject or content of sensitive or confidential data publically, or via systems or communication channels not controlled by . For example, the use of external e-mail systems not hosted by to distribute data is not allowed.

5. Please keep a clean desk. To maintain information security you need to ensure that all printed in scope data is not left unattended at your workstation. Sample Data Security Policies 2
6. You need to use a secure password on all systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.
7. Terminated employees will be required to return all records, in any format, containing personal information. This requirement should be part of the employee onboarding process with employees signing documentation to confirm they will do this.
8. You must immediately notify in the event that a device containing in scope data is lost (e.g. mobiles, laptops etc).
9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform so that they can take appropriate action.
10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from if you are unsure as to your responsibilities.
11. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car. 12.
12. Data that must be moved within is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc). will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with . 13.
13. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from .