Perry Group Policy Guidelines

Last Updated: February 2019

Perry Group Consulting Ltd.

Contents

1. Introduction

1. About

This document provides an overview of Perry Group thinking around IT Policy, Standards and Procedures and Guidelines.

2. References

The contents of this document are informed by the standards set by the IT Governance Institute (ITGI), a branch of ISACA, and independent, non-profit global organization engaged in the development, adoption and use of globally accepted IT standards and practices.

In addition, the document utilizes the experience of the Perry Group who have worked with various public and private sector organizations for the last fifteen years, allowing them to build up knowledge of how these organizations develop and implement governance models.

3. Storage of Policy and Standards, Guideline and Procedure Documents

It is recommended that all policies, standards and procedures should be stored in a central repository, ideally online and accessible by the audience for each policy.

This central repository should facilitate version control for all documents and should include templates for the creation of new policies. Even better, the repository should have the ability to track who has viewed and signed off on individual policies.

2. Policies, Standards and Procedures Descriptions

1. Policies

1.1 Overview

Many organizations confuse policies by including procedures within them or calling a procedure a policy. The two should always be separated, as policies should not change frequently, whereas procedures may change for a variety of reasons, such as performance improvement or additional tasks.

1.2 What is a Policy?

A policy is a deliberate system of principles to guide decisions and achieve rational outcomes. A policy is a statement of intent and is implemented as a procedure or protocol. Policies are generally adopted by a governance body within an organization.

A policy should be clear and precise, should include relevant information, and be as concise as possible to ensure understanding and clarity.

A policy should be implementable and enforceable, meaning a policy that does not make sense or that nobody would or could follow would be impractical and a waste of time for everyone in the organization.

1.3 Types of Policy

In many municipalities, there are two types of policy: Administrative and Council.

Administrative

In this type of policy, the policy is developed by administrative staff, vetted by senior management and approved by an appropriate person or group, usually the Head of Department, CAO, or Senior Leadership Team. There is no requirement to go to Council for approval due to either the enterprise governance model, or that Council have no involvement with how the policy is to be managed.

Council

Some organizations require only certain types of policy to be approved by Council, while others require all policies to be approved by Council. You should check your organization’s typical approach before issuing any policies.

It is important to understand the type of policy model in place for your organization, and to determine the level at which approval is required for your IT policies.

1.4 Issue and Audience

There are two key questions relating to any policy:

1. What is the issue to be addressed?
2. Who is the intended audience? (Who must comply with the policy?)

1.5 Categories of Policy

We recommend that IT Policies should be broken down into the following categories:

1. IT Governance, Risk and Compliance policies.
2. Project and Change Management policies.
3. IT Procurement policies.
4. Service Availability policies, like disaster recovery (DR), business continuity (BC).
5. Acceptable Use policies, like an email usage policy or computer usage policy.
6. Information Security policies - focus on managing and protecting and preserving information (including personal information) belonging to the organization, which is generated by those employees in the course and scope of their employment.
7. Information Management policies - focus on managing data such as its retention and destruction.

1.6 Specific vs Overall Policies

We recommend an approach which clearly differentiates between issue-specific, operational policies, standards and procedures, each of which should be set forth in separate documents. However, one policy that covers several areas of acceptable use can be created in a combined document e.g. Acceptable Use of IT Policy. It is essentially several specific policies wrapped into one document directed at one intended audience (e.g. users).

1.7 Characteristics of Good Policies

They should be:

- Short and to the point
- In plain and understandable language
- Well structured
- Consistent
- In accordance with and in line with the latest laws and regulations
- Clear on what is permitted and what is not
- Specific, relevant and applicable to the target audience

1.8 What should be included in a Policy?

As already stated, a policy should be as concise as possible, but some information must be included to ensure the audience understands why the policy has been established.

1. A header with the policy name and number, who it affects, the date it was established and the date it will be reviewed, as well as who has approved this policy.
2. The purpose of the policy. The audience must understand why the policy has been established, so providing a clear purpose is a necessity.
3. The scope of the policy. While the general audience is defined in the header, this is where specifics are included. For example, are volunteers or third-party contractors affected by this policy? Are there exceptions? Clearly state to whom the whole policy applies.
4. The statement. The statement is the actual rule or rules, standard or standards, that the policy needs to communicate.
5. The owner of the policy: who is responsible for maintaining this policy?

6. Definitions. Clearly define any terms used within the policy.
7. Legislation considered when developing the policy. State any legislation that was considered when developing the policy, and why it was considered.
8. The person or persons to whom questions regrading the policy should be directed.
9. References. Provide references to other documentation that support the policy, including other policies and any associated procedures.
10. Compliance requirements and penalties for non-compliance

2. Procedures

2.1 What is a Procedure?

A procedure is a document written to support a policy statement. A procedure is designed to describe who, what, where, when, and why in support of the implementation of a policy.

2.2 What should be included in a Procedure?

The procedure document should contain clear and precise information on how to complete the series of tasks that define the procedure.

1. A header with the procedure name and number, who it affects, the date it was established and the date it will be reviewed, as well as who has approved this policy.
2. The policy that the procedure is associated with.
3. Scope and applicability. Describe the purpose of the procedure, standards, and any regulatory requirements.
4. Roles and responsibilities. Describe who is responsible and what they are responsible for.
5. Desired outcomes. Describe what will happen when the procedure is completed.
6. Definitions. Clearly define any terms used in the procedure
7. Health and safety. Provide any health and safety warnings that may affect this procedure.
8. Equipment and supplies. Provide a list of equipment and supplies that may be required to complete the procedure.
9. Methodology and procedure. This is where you describe the tasks performed to complete the procedure. Use a series of numbered and sequenced steps. Include any ‘what if?’ considerations and what to do if situations are encountered.

3. Maintenance

3.1 Maintaining Policies

Policies should be reviewed on a regular basis to ensure they are still accurate, applicable and enforceable. Policies by nature should not change frequently. However, various factors may affect your policies and cause changes to be made.

For example, new legislation may take effect, or a Council may change and take a different strategic direction that would require an organizational policy change.

Policies should be reviewed at the very least bi-annually, and preferably annually.

3.2 Policy Disposal

In addition to policy maintenance, it may ne necessary at times to dispose of a policy. For example, a policy that states that confidential files must not be removed from the municipal building or network may become obsolete in today's world. The use of USB keys, Dropbox and other technologies result in a policy such as this being impossible to enforce, and also may be limiting performance and efficiency within the organization.

As such, it may be time to retire this policy. It could however be replaced with a new policy, stating that the confidentiality of these files must remain a priority and it is the responsibility of the staff member to ensure that confidentiality is maintained.

3.3 Communication of Polices

A consistent and effective way of communicating policies to their intended audience must be in place. This includes new policies, policy updates and changes as well as when policies are disposed of.

It is paramount that the audience for the policy be informed on the policy, and their responsibilities with regards to the policy.

3.4 Policy Sign-Off

It is recommended to have the audience members sign off on policies, to acknowledge that they have read and understood it and will abide by it. This will ensure that if a violation of the policy occurs, the sign-off document can be referred to in case lack of knowledge of the policy is given as mitigation.

3.5 Onboarding

When new employees are hired, important policies should be provided at onboarding, along with an explanation of each policy and the responsibilities of the new hire. Sign-off on understanding of the policies should be obtained at this time.

3.6 Maintaining Procedures

Procedures may change more frequently than policies. For example, someone may discover a better way to perform the procedure. Regulatory requirements may change requiring procedural changes.

Due to the potential of such changes, documented procedures should be updated as soon as a change in procedure is required. Ensure the procedure is tested against the documentation to ensure accuracy and effectivity.

Additionally, procedures should be reviewed annually to ensure they are still applicable and effective.

3. Policy Framework

1. Standards, Design and Content

There is no security policy standard and no general consensus as to what policies or how many should be in place, nor is there general consensus on policy design or content. Some organizations have a single generic document which combines policy, guidelines and standards (the combination approach), while others have multiple policies, guidelines and standards documents.

We recommend an approach which clearly differentiates between issue specific, operational policies, standards and procedures, each of which should be set forth in separate documents. The need to clearly differentiate between them is emphasised by the ISO 9000 Quality Standards for the preparation of internal documentation. For example, these ISO standards expressly state that policies must be separate and distinct from procedures.

1.1 Policies that are Successfully Implemented:

- follow a document hierarchy;
- take into account the organization's own identified risks and business needs;
- put in place a set of information security measures to demonstrate that the organization exercised due care and was not negligent;
- are compatible with the organization's culture and are thus more likely to be accepted and supported;
- are aimed at different audiences; and
- are kept up to date.

1.2 Document Hierarchy

Typically, such a framework would include a document hierarchy that includes the following:

Charter: (or mission statement) a concise document positioned at the top of the hierarchy that forms the capstone of the policies and presents the organization's philosophy of information security and establishes a management mandate for and commitment to implementing that philosophy;

Policies: There should be issue specific, operational policies that apply to specific issues (see the types of policies) and domains (for example applications, business units and regions) that must be complied with by all persons accessing these domains and to whom the issues apply;

Standards: these specify mandatory, uniform uses of specific technologies, configurations and procedures;

Procedures: provide detailed steps (sometimes in the form of a checklist) to be followed to achieve a particular recurring task (for example assigning appropriate privileges, running daily backups and updating firewall rules);

Guidelines: provide additional (optional) advice and support for policies, standards and procedures, as well as general guidance on issues such as how to secure systems, what to do in particular circumstances etc.

1.3 Audience-driven approach

Generally, policies are directed at several significantly different audiences because each audience has distinctly different needs.

For example, with end users, the focus is generally on acceptable use. But who is an end user? Is it permanent employees only or does it include people on fixed term contracts? What about suppliers?

With technical staff the focus is in much more detail, such as how to carry out the monitoring of a user email inbox or how to respond to a security incident or privacy breach. Separate documents should therefore be addressed to separate audiences so that the relevant audience is provided with only the information that is relevant to them. People need to only read those policies that directly apply to their own job.

Some policies are also directed at customers or management.

1.4 What Constitutes a Successful Policy Implementation?

Generally, issue-specific policies are easy to read, easy to rely on, easy to implement, easy to manage, easy to implement and easy to rely on in a court of law:

Easy to read: In the fast-paced information economy in which we live, people are pressed for time and will generally only read things that are relevant to them. The policies should therefore be in plain language and focused on particular audiences (typically end users, management and technical staff) addressing only those issues that are absolutely needed and that focus only on the essentials. Addressing a policy to multiple categories on readers makes it hard for the reader to find relevant information. For example, they might have to sift through a whole lot of rules before getting to the relevant rule relating to their email use.

Easy to rely on: With issue specific policies, it is easy accompany those policies with necessary guidelines or standards or procedures.

Easy to manage: Problems that arise tend to relate to issues and if those problems are recorded on an issue by issue basis, then it is easier to update the issue specific policies when reviewed annually.

Easy to implement: For purposes of education and awareness, issue-specific policies make it easier to convey key messages throughout the organization.

Easy to rely on in a court of law: One of the essential guidelines in cases of dismissal for misconduct for determining whether a dismissal or misconduct is unfair is whether or not the employee contravened a rule or standard regulating conduct … the rule was a valid or reasonable rule or standard … the employee was aware, or could reasonably be expected to have been aware, of the rule or standard … the rule or standard has been consistently applied by the employer. It is not possible to demonstrate “validity “or “reasonableness“ if the relevant “rule or standard” is found in a guideline (which is optional) rather than an issue specific policy (which is mandatory). More importantly, however, is the fact that an employee might be able to raise the defence in a disciplinary enquiry that there was in fact no “rule or standard” as (if it is contained in the guidelines) the rule is merely optional and does not have to be followed

4. Policy Requirements

1. Requirement for Policies

Perry Group views policies as being in three categories:

- **Essential** – an organization cannot operate effectively without them
- **Recommended** – the organizations would operate more effectively with them
- **As required** – the organization may need a specific purpose policy to operate effectively

1.1 Essential Policies

Perry Group believes the following minimum set of policies is essential for IT Departments within municipalities:

- IT Governance Policy
- Acceptable Use of Technology Policy
- Information Security Policy
- Privacy Policy
- Change Management Policy
- Mobility Policy
- Cloud Computing Policy
- Backups/Restores Policy
- Disaster Recovery Policy

1.2 Recommended Policies

The following policies are strongly recommended by Perry Group:

- Protection from Malware Policy
- Physical Security Policy
- Access Control Policy
- Disposition of Technology Policy
- Remote Access
- Incident Response Policy
- IT Procurement Policy
- Encryption Policy (Databases, mobile devices, etc.)
- Third-Party Remote Access Policy (vendors and support organizations)
- Data Management and Data Sharing Policy

1.3 As Required Policies

The following policies may be required to address specific issues or purposes within the organization:

- BYOD (Bring Your Own Device) Policy
- Social Media Policy (Possibly owned by Corporate Communications)
- Applications Usage Policy (Which existing systems should be looked at as a solution before purchasing new systems?)

- Website Policy (Who can create a website? Single corporate website only?; who approves?)

5. Policy Creation and Contents

1. What should be in each Policy

This section describes what we believe should be included in each individual policy.

1.1 Essential Policies

1.1.1 IT Governance Policy

This is an overarching policy that outlines how IT decisions are made. The following items should be included in an IT Governance Policy:

- How technology decisions are made
- Assignment of roles and responsibilities to bodies and individuals
- Project intake, review and approval process
- Architecture
- Policy, standards, guidelines and procedures

1.1.2 Acceptable Use of Technology Policy

- Corporate use of Internet and Email
- Personal Use of Corporate Technology including Internet and Email
- Computer, Email and Internet Monitoring
- Use of Social Media
- Procurement of Technology
- Installation of Software on Corporate Technology
- Use of Mobile Devices
- Using Personal Mobile Devices for Corporate Purposes

1.1.3 Information Security Policy

- User Account Management
- Access Control
- Password Requirements
- Sharing of User Accounts and Passwords
- Protection from Malicious Software
- Remote Access
- Physical Security
- Security Incident Response
- Mobile Device Management

1.1.4 Privacy Policy

- Privacy Statement on Sharing of Information
- Management of Personal Information including retention and Disposal
- Management of Personal Health Information (if appropriate)
- MFIPPA Requirements

1.1.5 Change Management Policy

- Definition of Change and when Policy Applies
- Change Approvals – Roles and Responsibilities
- Communications of Changes
- Time Periods for Changes
- Testing and Implementation Requirements

1.1.6 Mobility Policy

- Sourcing of Mobile Devices
- Approved Devices
- Eligibility
- Approvals

1.1.7 Cloud Computing Policy

- Approvals
- Host requirements for privacy, security, service levels
- Applicable laws and regulations

1.1.8 Backups/Restores Policy

- Types of Backups to be performed (Tape, Snapshots etc.)
- Frequency of Backups (Daily, Weekly etc.)
- Location of Backups (offsite etc.)
- Who can access?
- Restoration
- Continuity (Data formats must match current and future technology)
- Archival

1.1.9 Disaster Recovery Policy

- The Requirement for a DR Plan
- Frequency of Testing of the Plan
- Procurement for Replacement Equipment
- Requirement for a DR Facility

1.2 Recommended Policies

1.2.1 Protection from Malware Policy

- Responsibility
- Devices that must have anti-malware installed
- Specifics around Ransomware (pay ransom, etc.)
- How protection will be implemented
- Frequency of updates
- Exemptions/exceptions
- Licensing and Maintenance

1.2.2 Physical Security

- Locations and Facilities to be Secured
- Methods of security (swipe cards etc.)
- Who has access?
- Visitors to Facilities
- Emergency Procedures

1.2.3 Access Control Policy

- Who approves access?
- How access will be requested and granted
- Segregation of Duties
- Revocation of Access

1.2.4 Disposition of Technology Policy

- Types of Technology
- Disposition of Data
- Level(s) of Data Erasure
- Retention of Data (Is data on device still required?)
- Sale of Technology Equipment

1.2.5 Remote Access Policy

- Security Requirements
- Qualifications for Access
- Third-party and Vendor Access
- Personally-owned equipment requirements

1.2.6 Incident Response Policy

- Who is accountable?
- Roles and Responsibilities
- Communications Plan
- Incident Handling and Reporting
- Legislation around security breaches

1.2.7 IT Procurement Policy

- Software Procurement
- Hardware Procurement
- External Services
- Exceptions and Restrictions

1.2.8 Encryption Policy

- Database Encryption Standards
- Mobile Device Encryption Requirements
- Mobile Device Encryption Standards

1.2.9 Third-Party Remote Access Policy

- Which vendors can access which systems?
- Logging of vendor sessions

- Monitoring of vendor sessions
- Access controls such as multi-factor authentication

1.2.10 Data Management and Data Sharing Policy

- Who is responsible for/can manage data?
- Who is responsible for setting data standards?
- What data/types of data can be shared?
- Who approves data sharing?

1.3 As required Policies

1.3.1 BYOD Policy

- Supported Devices
- Password Requirements
- Supported Applications
- Responsibilities for payments
- Security levels applied by the organization to personally-owned devices
- Employee termination requirements
- Expectation of Privacy
- Liability

1.3.2 Social Media Policy

- Who is responsible to represent the organization on Social Media?
- Guidelines on what can be shared
- Social Media for Organization
- Social Media for Personal Use
- Etiquete
- Confidentiality

1.3.3 Application Usage Policy

- List of core systems
- Request/Approval process to use existing system for new purpose
- Request/Approval process to purchase a new system

1.3.4 Website Policy

- Is the corporate website the only website?
- Can individual departments create their own websites?
- Request/Approval process for a new website or addition to existing website

6. Standard Creation and Contents

Standards are put in place to ensure that all members of an organization are working within the same parameters. This may be to ensure that technology can be managed effectively for example, as a single set of technologies could be a standard rather than allowing multiple technologies to be implemented.

1. Technology Standards

Technology standards is a generic term for standards related to technology and include such things as:

- Software Platform Standards
- Architecture Standards
- Information/Data Standards
- Information Technology Service Management
- Environmental Standards
- Networking Standards
- Security Standards
- Enterprise Product Standards

1.1 Software Platform Standards

This standard lists IT software products being deployed within the standardized IT development, test and deployment environments.

1.2 Architecture Standards

- Target Enterprise Architecture
- Application Development Standards (if appropriate)
- Network Architecture Standards
- Server Platforms

1.3 Information/Data Standards

- Address standards and other information used across platforms and systems
- Web Metadata Standards
- Date Formats
- Geospatial Data Standards

1.4 Information Technology Service Management Standards

- Standard to be used (ITIL for example)
- Change Management Standards
- Incident Management Standards
- Problem Management Standards
- Service Level Management

1.5 Environmental Standards

- Acquisition of Electronic Equipment
- Printing and Copying
- Power Management

1.6 Networking Standards

- Firewall Standards
- Wired Networks
- Wireless Networks

1.7 Security Standards

- Firewalls, Routers and Switches
- Wireless Networks
- Remote Access
- Server Hardening
- Mobile Devices
- Web Applications
- Cloud Standards
- Physical Security
- Device Disposal Standards
- Patch Management

1.8 Enterprise Product Standards

- Network Operating Systems
- Desktop Operating Systems
- Database Systems
- Business Intelligence Systems

1.9 Creating a Standards Document

A Standards Document should include the following:

- Scope – what does the standard refer to and what does it affect?
- External References – list external references such as ISO, IEEE etc.
- Internal References – list any internal references such as policies
- Terms and Definitions
- Standard – describe the standard

7. Procedure Creation and Contents

1. Associated Procedures

Many policies should have procedures that are associated with them. This section will identify some of the procedures that should accompany each of the respective policies.

1.1 Acceptable Use of Technology Policy

- Procurement of Technology Procedure
- How to access the network using a mobile device
- How to get access to the network from your personally-owned device

1.2 Information Security Policy

- How to request a new user account
- How to revoke access for a terminated employee
- How to change your password
- How to request Remote Access
- How to report a Security Incident

1.3 Privacy Policy

- How to report a privacy breach

1.4 Change Management Policy

- Change Management procedures
- Change Management window

1.5 Mobility Policy

- How to request a mobile device
- How to request network access from a personally-owned device
- How to report the loss of a mobile device

1.6 Cloud Computing

- How to request a new cloud service
- How to access a cloud-based system
- How to determine host security and privacy capabilities

1.7 Backups Policy

- Backup procedures
- Frequency and type
- Restore procedures
- Offsite backups storage procedures
- Security for file restores (user verification)

1.8 Disaster Recovery Policy

- Disaster recovery Plan
- Disaster recovery testing procedure

1.9 Disposition of Technology Policy

- Disposition Procedures
- Data Retention Procedures

1.10 IT Procurement Policy

- Corporate Procurement Procedures
- How to procure new hardware/software