CORE
CONCEPT
SECURITY

Froud on Fraud

SECURITY IS NOT EASY, BUT IT CAN BE SIMPLE.

White Paper

Choosing the Right Policy Set
(...and the right vendor to deliver it.)

By: David Froud

Date: February 6, 2017

SUMMARY

There are only 4 Foundations of Security. Regardless of your business's size, region, or industry sector, unless you have the following in place your security program will fail:

1. **<u>Management Buy-In / Culture</u>** - The vast majority of the responsibility for the security culture of any organisation falls firmly on the shoulders of the CEO (or equivalent).

Unless your company IS a security company of some sort, security is an expense, and whether or not that expense is seen as a business enabler (which it is) depends on the CEO's attitude towards it.

The remaining foundations have little chance of success unless you get this one right.

2. **<u>Policies & Procedures</u>** - It's amazing how many people groan at this, and even security professionals cringe at the 'paperwork' they have to troll through.

That's a shame really, because without that paperwork, you will never HAVE security. It's your company's instruction manual for how to do what you do, properly, responsibly, and *securely.* Anyone who's put together a chest of drawers from Ikea knows exactly what I mean; maybe, and I mean MAYBE, you could work it out for yourself, but how much more painful would that be? It's bad enough WITH the instructions!

Your policies and procedures let all employees know what to do, and as importantly, what NOT to do. It's enough that the thieves want to steal your data, why make things worse by not preventing your own employees from giving it away!?

3. **<u>Governance</u>** - Few phrases in security are perceived to be more ambiguous, open to interpretation, or complicated.

Wikipedia says; "*Information Technology Governance is a subset discipline of corporate governance focused on information technology (IT) systems and their performance and risk management.*"

I can simplify this to; "IT Governance is the business side and the IT side having *meaningful* conversations."

It does not have to be complicated, it just has to be appropriate. You don't have to hire additional people to run it, you just have to assign the tasks, responsibilities, and accountability.

4. **<u>Education & Training</u>** – Self-explanatory, I hope.

The Policies are arguably the most important of the 4, as without them, there can <u>be</u> no foundation on which to build the remaining program.

ADDRESSING THE CHALLENGE

First, you must define each of the document types you are creating:

- **"Policy"**: Organisation-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures. In other words the DOS and DO NOTS of expected behaviour. Typically consist of language like; must and must not, shall and shall not etc. Contents are mandatory.

- **"Standard"**: Specific requirements and parameters of operation for the organisation. Standards define _exactly_ what something must look like. From operating systems, to network devices, to application & software, this is how they will be configured.

- **"Procedure"**: Descriptive narrative for a Policy. Procedure is the "how to" for a Policy and describes how the Policy is to be implemented. Often, Procedures will be step-by-step instructions on how to perform a specific action. As such they represent the sum of almost all corporate knowledge as it relates to the running of a security program.

- **"Guidelines"**: A non-mandatory good practice, often use to help less experienced individuals meet the intent of the above documents.

Second, you need someone to run the project internally (a Policy Coordinator), and likely an external consultant to provide the necessary expertise to ensure the Policy Set stays appropriate to the business culture and goals. If regulatory compliance is a big driver, you will need to choose a consultant with sufficient expertise.

Third, you must define the documents required. Up front. If you already have some documentation, you'll only be looking to fill the gaps. But if you're starting from scratch, you need to choose a Policy Set of _appropriate_ depth and breadth. Most vendor supplied Policy Sets are designed with large business in mind, meaning the vast majority of the content will need to be adjusted or even removed altogether.

Fourth, define how the resulting Policy Set will be managed moving forward.

- o Do you have an Intranet on which these documents can be distributed?
- o Would a Document Management System (DMS) make more sense?
- o Do you have an online training platform that can be used to not only distribute the Policy Set, but train employees in their use?
- o Can HR add these documents to both the on-boarding process and the ongoing awareness training curriculum?

And lastly, distribute the ongoing review and maintenance of every document to the role best qualified to do so. If you have a IT governance function, add the Policy to their list of responsibilities.

WHAT'S IN A POLICY SET?

Depending on the size and complexity of an organisation, there can be a few dozen to several hundred documents. However, the following _should_ be part of every Policy Set regardless of organisation size, region, or function:

Mandatory Polices[*]

- **_Information Security Policy Framework (ISPF)_**: The ISPF is the overarching document of the Policy Set and sets the tone for everything that comes after it. The most important sections will include:

  - _IS Role & Responsibilities_ - Who is supposed to do what, from the CEO down to the most junior employee.

  - _Documentation Development_ - Makes the Policy Set mandatory.

  - _Policy Format / Naming Conventions_ - Standardises all document content.

  - _Policy Exceptions_ - There will always be times when you cannot perform something in-line with your polices, but this must be approved and tracked accordingly.

  - _Change Management_ - Makes this mandatory.

- **_Acceptable Use Policy (AUP)_**: Not every policy is appropriate to distribute to every employee, but there are some things that must be enforced across the board. The AUP - often called the Code of Conduct (CoC) – sets out those things that are to be followed by everyone, form the Board of Directors (BoD) to external consultants.
  The AUP End User Agreement is signed by every employee and a copy of that signature must be held on file.

- **_Data Classification Policy_**: No Policy Set is complete without data classification, as every other policy will in some way refer to it, and or be labelled _with_ it. There can be no appropriateness in security until you've baselined your controls to the risk.

- **_Business Continuity Policy_**: Not much point being in business if you don't make _staying_ in business a mandatory requirement.

- **_Risk Management Policy_**: This can include everything from mandatory risk assessments, to incident response and disaster recovery. Regardless of what it contains, the risk management policy requires the organisation to measure its risk in a standardised fashion and mitigate that risk appropriately.

Mandatory Standards[†]

- **_Document Management Standard_**: From numbering, to style/format, to content, what goes into a document must be fully defined.

---

[*] _Note: Lists of the most common Polices can be found at Annex A_
[†] _Note: Lists of the most common Standards and Procedures can be found at Annex A_

- **Asset Registration Standard**: Asset management is the centre of every security process. From risk assessments, to vulnerability management, if you don't know what you've got, you can't protect it.

- **Configuration Standard(s)**: Every asset must be installed in a manner that supports one of the tenets of security; least privilege. Configuration standards are the only way to ensure that security in built in from the beginning, and how security is maintain throughout an asset's entire life cycle.

Mandatory Procedures

- **Document Management Procedure**: How the Policy Set is to be managed and maintained.

- **Change Control Procedure**: Nothing in an organisation should change without explicit permission. How that change is effected without creating a bottleneck and who can approve changes is defined in this procedure.

- **Policy Exception Procedure**: In reality it is impossible to conduct a business within the confines of the policy statements. However, that is no reason for performing any action outside of the _scope_ of a Policy Set. The exception process is the official way to continue performing a function with full oversight into the risk of doing so.

- **Incident Response Procedure**: No point being in business if you don't intend _staying_ in business. Robust incident response procedures are about the only way you can prevent a security event - which _will_ occur - into a business crippling disaster.

- **Disaster Recovery Procedure**: Inevitably, things will go wrong. Organisations that can get back on their feet faster stand a better change of fully recovering. This procedure, or more likely procedures, should fully define how to get every business process back online.

- **Security Training & Awareness Procedure**: What must everyone in your organisation know in order to fully support / enable the business goals? As one of the 4 Foundations of Security a well-defined procedure is critical the success of any security program.

ASK FOR WHAT YOU NEED

The questions below are designed to be generic enough to suit almost any business, as well as form the core questions in your Request for Proposal (RFP);

1.   On which information security framework or frameworks is the Policy Set based?

   Regardless of the reason you require a policy set - to achieve Payment Card Industry (PCI) compliance for example - your policies should be based on an industry acceptable framework for the management of a security program. There are several; Control Objectives for Information and Related Technology (COBIT), NIST SP 800 Series etc., but it's the ISO 27000 Series that has been dominant globally for much of the last decade.

   Other than PCI, no other regulatory compliance regime on the planet that we have seen makes any of these frameworks mandatory, but it just make sense to choose the most common and map your policy set to it. Many organisations have mapped the other frameworks to ISO 27001, so it should be a simple process to obtain these if required. Whatever your requirement, make sure you choose a policy set that meets not only your immediate compliance needs, but the needs of your business across the whole relevant regulatory landscape.

2.   Can you provide a list of included policies?

   No policy set can ever include completed Standards or Procedures, these are entirely unique to an organisation, but the Policies should cover just about any business with a little customisation. Assuming the Policies have been mapped to an appropriate framework, deciding how the Polices should be amended should be very straightforward.

   The better policy sets will include every policy statement an organisation could possible need, along with the context for its inclusion or exclusion.

3.   Does your service include a mapping of policy statements to the PCI DSS?

   While this question seems to be a little specific, no other compliance regulation in history has driven the need for commercially available policy sets quite like PCI. It therefore makes sense that, at a minimum, all relevant policy statements are mapped to the PCI DSS out of the box.

   Ideally, there will be three mappings:

   i.   *All policy statements mapped to the PCI DSS v3.2 (as stated above);*

   ii. *The PCI DSS v3.2 mapped to all policy statements as well as all Standard / Procedure templates; and*

   iii. *The PCI DSS v3.2 Report on Compliance template mapped to all policy set templates.*

   Compliance with PCI is almost 40% 'paperwork', if you're going to invest in a Policy Set you want this work done for you.

4. Does your service include a mapping of policy statements to ISO27001 (or whatever Information Security framework you used)?

Similar to the PCI question above, there's little point in purchasing a policy set if it's not already mapped to the framework upon which you have based, or will be basing, your entire security program.

Only an appropriate mapping of the policy statements to your chosen framework allows you to determine the impact of your customisation process. You must have this appropriate context or your policy set may not support your regulatory compliance efforts.

5. Can you provide a Document Management Standard and Procedure?

One of the biggest drawbacks of buying a policy set is that few people have the necessary skill-set to maintain it once the vendor has completed the initial customisation. Policies, Standards and Procedures must be constantly reviewed for validity, amended in response to internal and external influences, and distributed to everyone with a need to know.

Well-documented management standards and procedures allow organisations to keep their policy set relevant, and if required, compliant. No organisation should ever rely on a 3rd party to maintain their paperwork (see Question 12).

6. *Do you provide an Information Security Governance Charter template?*

The word 'Governance' is usually enough to put organisations off altogether. Surely only large organisations need something so 'official'? Nothing could be further from the truth. IS Governance is where the business side and the IT have meaningful conversations about how to achieve the business's goals. It is therefore perfectly placed to be responsible for the policy set. The challenge for most organisations is where to start.

A well-written and appropriate Governance Charter is often all organisations need to overcome their inertia, whatever the cause.

7. Do you provide document templates for the most common Procedures and Standards?

Any vendor offering a Policy Set that includes drafts of every Standard and Procedure is often nothing more than snake oil. Both Standards and Procedures are totally unique to each organisation, and can never be entirely relevant out of the box.

That said, every document in a policy set has standardised content headings; e.g. 'Objective' / 'Scope' / 'Document Management' etc. These templates can all be drafted based on most common content and established usage. The most any vendor can provide are templates for all the most common Standards and Procedures, as well as examples of the ones a little more difficult for the inexperienced to understand (see Question 8).

8. Can you provide best practice samples of the more common procedure / standard documents?

Per Question 7. above, only the Policies can truly contain relevant content out of the box. However, there are several procedures where client specifics will be built on a standard framework.

For example, the following Procedures are all predicated on a chosen best practice framework:

i.   Document Management Procedure

ii. Risk Assessment Procedure

iii. Incident Response Procedure

So while the full specifics will be customised to the individual organisation, the guidance related to these more difficult concepts in the form of examples can be invaluable.

9.   Do you include an instruction manual to enable self-customisation?

Many commercially available policy sets are based on Microsoft Word templates. While there is nothing wrong with that, few come with an instruction manual on how to customise them to meet your existing brand requirements.

This gap often forces organisation to purchase additional consulting time to perform this relatively simple task, so the better Policy Sets will include a manual to allow you to customise the entire thing yourself.

There are online versions of the policy set service, but you will need to be very careful in choosing one of these options as internal distribution of the results can be troublesome. Again, you must define your needs first, then choose the right option for you.

10. Can you scale your consultancy offering to include a fully bespoke Policy Set?

The development of a policy set may be relatively simple to those already with the skill-set, but it can look extremely complicated to a non-security expert. There is therefore little point in a vendor offering a policy set without having the necessary consulting skill-sets backing them up to actually deliver a final product.

However, this service should be entirely scalable and bespoke to each organisation's needs. If all that is required is a few polices to fill the gaps in existing documentation, then the consulting service should adapt. If an organisation requires every document from scratch, then the service must include a significant level of guidance to enable self-sufficiency when the consultant is through.

11. Do you provide your policy set in other languages?

The vast majority of vendors will only provide policy sets in English, so if you have language requirements you must ask up front. And get samples, Google Translate will not get the job done.

The alternative is a translation service. It's possible a vendor has existing relationships to get this done cheaper, but you should still do your own homework.

12. Can you help us manage this moving forward?

As stated previously, no policy set service should involve an ongoing relationship that includes maintaining the entire documentation management program. You don't brush your children's teeth every day, you teach them how to do it for themselves.

That said both the prevailing threat landscape and the regulatory landscape are in constant flux. Therefore, vendors offering an ongoing advisory service, even under a paid retainer, are providing a more sustainable offering.

13. What if we fail to achieve compliance with our chosen regulation?

No policy set vendor can guarantee compliance first time around. Compliance with any regulation is almost entirely predicated on the interpretation of an auditor/assessor, each with their own unique biases.

However, if you write the achievement of compliance into the contract as an SLA, you can ensure that the vendor makes the necessary adjustments per the assessor's findings. At least for the Policies.

14. Monolithic vs. Modular

While this is largely a matter of preference, monolithic policy sets tend to be extremely difficult to manage. Assigning ownership to a document section, as well as recording version history, are next to impossible unless each subject is a stand-alone document.

Distribution and awareness also become an issue when the vast majority of a monolithic security policy's content is irrelevant to most employees.

It is also my experience that most monolithic policies were written to scrape through some some kind of compliance requirement, PCI being the most common offender. If a policy set is only seen in this light you may as well get the cheapest.

15. How long does the process take?

Basically a trick question, there are way too many dependencies on the client side for any vendor to estimate how long the service will take. However, any additional consultancy should be valid for at least 1 full year as that's how long it could take to get the program in place. Assuming of course that it's implemented correctly.

SUMMARY

Choosing a policy set can seem complicated at first, especially if you do not have a security specialist on staff. However, if you keep the following points in mind, and ask all the questions above, you should be able to choose the right policy set for your business goals, whatever they may be;

1. At a bare minimum, get the CEO to sign the ISPF. If you can't get him/her to accept the accountability for security in this limited fashion the rest of the program will be seen as nothing more than a burden;

2. Policies must be a reflection of your existing corporate culture, not a radical shift in response to some external compliance requirement;

3. Policies should always be aspirational in nature, otherwise continuous improvement is next to impossible;

4. As a corollary to 2., use the exception process to record everything you are NOT doing relevant to your policies. These are the first entries onto your risk register;

5. Assign all Policies to the highest level and to the most appropriate role in your organisation. While these individuals may not actually write the content, they should be fully accountable for its distribution and enforcement;

6. Assign coordination of all Standards and Procedures to the SME most suited to do so; and

7. Work closely with an independent body (Internal Audit or equivalent) to ensure that the policies are appropriately enforced.

In the end, choosing the right policy set is dependent on why you're buying one in the first place. If it's just for PCI compliance only, then you might as well by the cheapest and crappiest offering out there, nothing will help you be secure.

If, however, you actually care about security, _and_ recognise the enormous benefit a good security program can bring to the business, then you really need to do your homework.

No, it will not be cheap, but you'll get what you pay for.

ABOUT FROUD

David Froud has been implementing security programs into organisations large and small for much of the last 20 years.

David's proprietary Policy Set has ensured the clients received the business benefit required for both ongoing security and compliance.

For more information;

Blog:　　　　http://www.davidfroud.com

Linkedin:　　　http://www.linkedin.com/in/davidfroud

ANNEX A - MOST COMMON POLICY SET DOCUMENTS

Policies:

- Information Security Policy Framework
- Acceptable Use Policy
- Acceptable Use Policy-End User Agreement
- Data Classification Policy
- Data Handling & Media Destruction Policy
- Data Retention and Role Access Policy
- Asset Management Policy
- Business Continuity Management Policy
- Access Control Policy
- Remote Access Policy
- Risk Management Policy
- Incident Response Policy
- Disaster Recovery Policy
- Vulnerability Management Policy
- Security Awareness & Training Policy
- Cryptography & Key Management Policy
- System Configuration & Maintenance Policy
- Network Configuration Policy
- Secure Application Development Policy
- Use of Critical Technologies Policy
- Vendor Management & Due Diligence Policy
- Telecommuting & Mobile Computing Policy
- Physical Security Policy
- Privacy & Regulatory Compliance Policy

Standards:

- IS Document Management Standard
- [DESKTOP-LAPTOP] Configuration Standard
- [FIREWALL-ROUTER] Configuration Standard
- [IDS-IPS] Configuration Standard
- [OPERATING SYSTEM] Configuration Standard
- [WIRELESS ACCESS POINT] Configuration Standard
- Asset Registration Standard
- Authentication Standard
- Logging & Monitoring Standard
- Penetration Testing Standard

- Software Development Life Cycle
- [PHYSICAL SECURITY] Standard
- Encryption & Key Management Standard
- Network Time Synch Standard

Procedures:

- IS Document Management Procedure
- Change Control Procedure
- Data Backup & Media Handling Procedure
- Data Destruction Procedure
- Encryption & Key Management Procedure
- Firewall-Router Change Request Procedure
- Incident Response Procedure
- Log Review & Monitoring Procedure
- Disaster Recovery Procedure
- Periodic Security Operations Procedure
- Risk Assessment Procedure
- Rogue Device Detection Procedure
- Security Awareness Training Procedure
- User Access Request Procedure
- Vulnerability Management Procedure
- Vendor Due Diligence Procedure
- Policy Exception Procedure
- Asset Registration Procedure
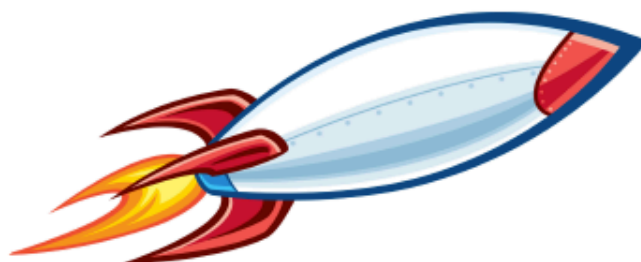- Software Approval Procedure

Other:

- New Policy Template
- New Procedure Template
- New Standard Template
- Governance Steering Committee Charter
- Master Document Register
- Policy Master & Compliance Mapping
- Document Template User Guide

ANNEX D - SAMPLE REGULATORY / FRAMEWORK MAPPING

Policy Statement Mapping

ACME ROCKETS							
Policy#				**ISO 27001**	**DSS #**	**DSS Requirement Description**	**Related Policy(ies) / Procedure(s) / Standard(s)**
POL002		**Acceptable Use Policy**					
POL002	2.1	**Acknowledgement of User Responsibilities**	All users must review and acknowledge their understanding of the *[DOC_NUM] - Acceptable Use Policy* (this policy) and other related information security policies on an annual basis.	A.07.02.01	12.4.a	**12.4.a** Verify that information security policy and procedures clearly define information security responsibilities for all personnel.	
POL002	2.2	**Assets and Intellectual Property**	All information systems assets provided by [COMPANY_NAME_ABRV] remain the sole property of [COMPANY_NAME_ABRV]. Any data or intellectual property created by the user remains the property of [COMPANY_NAME_ABRV] and should not be removed, copied or shared with any person or entity except as part of the user's normal job responsibilities. Intellectual Property includes, but is not limited to; patents, copyrights, trademarks, and material such as; strategic plans, products, computer programs etc.	A.18.01.02	12.3.10.a	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	[DOC_NUM] - Use of Critical Technologies Policy
POL002	2.3	**Monitoring**	Where allowed by law, [COMPANY_NAME_ABRV] reserves the right to monitor all activities that occur on its electronic assets, whether on [COMPANY_NAME_ABRV] owned or leased systems, or on any other permitted devices used for [COMPANY_NAME_ABRV] work purposes.	A.07.02.01	10.1	**10.1** Verify, through observation and interviewing the system administrator, that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users.	[DOC_NUM] - System Configuration & Maintenance Policy [DOC_NUM] - Incident Response Policy
POL002	2.4	**Access to Data**	Where allowed by law, [COMPANY_NAME_ABRV] reserves the right to access any data that resides on its electronic assets, whether on [COMPANY_NAME_ABRV] owned or leased systems, or on other permitted devices containing [COMPANY_NAME_ABRV] data assets.	A.07.02.01			
POL002	2.5	**Moving, Copying, and/or Storage of Information Assets**	Unless protected by security controls at least equal to those enforced internal systems, and explicitly approved by the relevant Data Owners, it is prohibited to move, copy, or store data above classification level [DATA_CLASSIFICATION] on local hard-drives, or removable electronic media. Further, all information assets will be protected (at a minimum) to any applicable Industry Standard or Regulation as defined in the *[DOC_NUM] - Data Handling & Media Destruction Policy*.	A.07.02.01	12.3.10.a 12.3.10.b	**12.3.10.a** Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies. **12.3.10.b** For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.	[DOC_NUM] - Data Classification Policy [DOC_NUM] - Data Handling & Media Destruction Policy [DOC_NUM] - Data Retention and Role Access Policy
POL002	2.6	**Role and Function**	Use of [COMPANY_NAME_ABRV] electronic assets must be consistent with the individual's role within the organization and intended function of the asset.	A.07.02.01	7.2.2 12.3	**7.2.2** Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function. **12.3** Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed:	[DOC_NUM] - Access Control Policy
POL002	2.7	**Unacceptable Use**	Using [COMPANY_NAME_ABRV] electronic assets for abusive, unethical, or inappropriate purposes will not be tolerated and may be considered grounds for disciplinary action, including termination of employment for gross misconduct. Unacceptable use of electronic assets includes, but is not limited to: • the transmission of any [COMPANY_NAME_ABRV] data above [DATA_CLASSIFICATION] unencrypted over end user messaging technologies, including - but not limited to – email, instant messenger, SMS, text etc. ...	A.13.02.03	4.2.b 12.3.5	**4.2.b** Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies. **12.3.5** Verify that the usage policies define acceptable uses for the technology.	
POL002	2.8	**Installation of Software Packages**	The installation of software packages not approved by [SOFTWARE_APPROVER] is strictly prohibited. Requests for approval shall be processed through the [SOFTWARE_APPROVAL_PROCEDURE]. Approved software list can be found here; [APPROVED_SOFTWARE_LIST].	A.12.06.02			

ANNEX E - SAMPLE POLICY

ACCEPTABLE USE POLICY

Revision: r1.0

Effective Date: 01-Jan-17

Classification: INTERNAL RESTRICTED

Regional Applicability: ALL

Departmental Applicability: ALL

Doc. Name:	ACCEPTABLE USE POLICY			Doc. Number:	ARL-POL-002
Revision:	r1.0	Status:	RELEASED	Effective Date:	01-Jan-17

1. Introduction

1.1 Document Definition

This document is a Policy.

For a full description of document types, see *ARL-POL-001 - Information Security Policy Framework*.

1.2 Objective

The objective of this policy is to outline the acceptable use of electronic and data assets at Acme Rockets Ltd. (ARL). Inappropriate use exposes ARL to risks including, compromise of network systems, services and data, negative commercial impact, and People / Legal issues.

Assets may include but are not limited to:

- Electronic Media
- Desktop and Laptop Computers
- Servers
- Network Infrastructure
- Telephones
- Fax Machines
- Mobile Computing and Communication Devices

1.3 Scope

1.3.1 Applicability to Staff

ARL refers to Acme Rockets Ltd. as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

1.3.1 Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

1.3.2 Applicability to Assets

This Policy applies to all information assets globally owned by ARL, or where ARL has custodial responsibilities.

1.4 Related Documents / References

- *ARL-POL-001 - Information Security Policy Framework*
- *ARL-POL-005 - Data Handling & Media Destruction Policy*
- *ARL-POL-003 - Acceptable Use Policy-End User Agreement*

Doc. Name:	ACCEPTABLE USE POLICY			Doc. Number:	ARL-POL-002
Revision:	r1.0	Status:	RELEASED	Effective Date:	01-Jan-17

- *ARL-PRC-ALL-ALL-002 - Change Control Procedure*

2. Policy Statements

2.1   Acknowledgement of User Responsibilities

All users must review and acknowledge their understanding of the *ARL-POL-002 - Acceptable Use Policy* (this policy) and other related information security policies on an annual basis.

2.2   Assets and Intellectual Property

All information systems assets provided by ARL remain the sole property of ARL. Any data or intellectual property created by the user remains the property of ARL and should not be removed, copied or shared with any person or entity except as part of the user's normal job responsibilities.

Intellectual Property includes, but is not limited to; patents, copyrights, trademarks, and material such as; strategic plans, products, computer programs etc.

2.3   Monitoring

Where allowed by law, ARL reserves the right to monitor all activities that occur on its electronic assets, whether on ARL owned or leased systems, or on any other permitted devices used for ARL work purposes.

2.4   Access to Data

Where allowed by law, ARL reserves the right to access any data that resides on its electronic assets, whether on ARL owned or leased systems, or on other permitted devices containing ARL data assets.

2.5   Moving, Copying, and/or Storage of Data Assets

Unless protected by security controls at least equal to those enforced internal systems, and explicitly approved by the relevant Data Owners, it is prohibited to move, copy, or store data above classification level CONFIDENTIAL on local hard-drives, or removable electronic media.

Further, all information assets will be protected (at a minimum) to any applicable Industry Standard or Regulation as defined in the *ARL-POL-005 - Data Handling & Media Destruction Policy*.

2.6   Role and Function

Use of ARL electronic assets must be consistent with the individual's role within the organisation and intended function of the asset.

Doc. Name:	ACCEPTABLE USE POLICY			Doc. Number:	ARL-POL-002
Revision:	r1.0	Status:	RELEASED	Effective Date:	01-Jan-17

3. Policy Compliance & Enforcement

3.1 Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

Criteria	Example Evidence
Evidence of users review and acknowledgement of their understanding of ARL Acceptable Use Policy and other related information security policies.	• New hire training user sign-off documentation • Electronic responses to periodic surveys or security awareness training
Evidence that users are complying with the concepts of acceptable use.	• Root cause analysis from periodic internal or external audit results

3.2 Enforcement

As noted above, this Policy applies to all Acme Rockets Ltd. employees, officers, members of the Board of Directors, and all consultants and contractors. Violations of this Policy may result in disciplinary action, up to and including termination of employment and / or legal action.

Doc. Name:	ACCEPTABLE USE POLICY			Doc. Number:	ARL-POL-002
Revision:	r1.0	Status:	RELEASED	Effective Date:	01-Jan-17

4. Exception Process / Glossary

4.1 Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *ARL-POL-001 - Information Security Policy Framework*.

4.2 Glossary / Acronyms

Junk Mail	Unsolicited mail sent out usually by direct marketing or direct mail firms. Used mainly for introducing new products, books and magazines, investment opportunities, merchandise catalogues, etc.
Spamming	Email spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

Doc. Name:	ACCEPTABLE USE POLICY			Doc. Number:	ARL-POL-002
Revision:	r1.0	Status:	RELEASED	Effective Date:	01-Jan-17

5. Document Management

5.1 Document Revision Log

Date	Editor	Revision #	Description of Change
15-Dec-16	R. D. Runner	0.1	Initial draft.
31-Dec-16	R. D. Runner	1.0	Final version.

5.2 Document Ownership

This Policy is owned by the General Counsel.

5.3 Document Coordinator

This Policy is coordinated by the HR Director.

5.4 Document Approvers

Approver Name	Signature	Date
Will E. Coyote / General Counsel	[Signature held on file.]	01-Jan-17