

C U T L A S S I N C .

# Security and Administration Guide

*27 November 2011*

*Owner: Steve Bull, [steve.bull@gmail.com](mailto:steve.bull@gmail.com)*

## Table of Contents

1.0	Introduction.....	3
2.0	Employment & Services Contracting Practices.....	3
3.0	Security Practices .....	4
3.1	Physical Security	
3.2	Technology Controls	
3.3	Administrative Controls	
4.0	Other Administrative Practices .....	5
4.1	Investment Administration	
4.2	Procurement	
4.3	Accounting	
4.4	Project Planning and Control	
5.0	Quality Practices .....	7
5.1	Configuration Management	
5.2	Software Development and Quality Assurance	
5.3	Risk Management	
6.0	Planning and Communications .....	8

### *APPENDIX*

1. Software & Document Naming and Management Protocol
2. 2011 Risk Assessment Methods and Results (Results not available in public version of this document)
3. Agreement Templates and Samples

## 1.0 Introduction

CUTLASS INC. (Cutlass) was founded in 2002 as a S Corporation in New York State, USA. Cutlass is a national provider of locative media, producing and distributing its own branded cell phone entertainment, as well as building commissioned custom wireless applications.

Cutlass' vision is to achieve excellence by being a customer-focused, high performance organization dedicated to improving the lives of our customers. Cutlass achieves business leadership through the ownership, urgency and accountability of our personnel.

Cutlass' commitment to excellence is fundamental to the philosophy of Cutlass. This commitment means that each one of us as an employee or affiliate of Cutlass shares a common set of objectives and benefit from the achievement of those objectives. As a developer of innovative, telephony based products, some of its efforts remain within the management domain of Cutlass, others are sold as ideas or proofs of concept. The following are a sampling of recent Cutlass products:

- SalesPitch™ (a stand-alone cell phone service for sales people)
- EZfollowups (spoken reports and reminders on mobile devices)
- SMS Time Card
- Citizen FYI
- Slavery In New York (cell phone tours)
- Hollywood USA
- PreMinder (currently under development)
- AZZA (DIY formula art for iPad, iPhone and Android devices)
- Pet-Pals
- Cutlass Treasure Hunts (1<sup>st</sup> person performance games on college campuses)

As a corporation primarily devoted to new technology products, projects at Cutlass are fast paced and very fluid in how they are funded, executed, and then brought to market. In its work, Cutlass is committed to being predictable to the community, fair to its affiliates, and responsible to the well being of the planet. Cutlass develops products for healthcare, mass transit and other industries regulated by HIPAA, DoT specifications and others. Cutlass understands the need for standard operating procedures and applies a risk-based, graded approach to placing and monitoring administrative controls on its work.

The purpose of this document is to summarize both the process and resulting controls that Cutlass has established to ensure excellence in its outputs. The document reflects the practices and methods used to produce PreMinder and other products at Cutlass. These practices ensure timely, quality products for Cutlass customers and sponsors. To ensure consistency and predictability, this document also serves as a training aid for Cutlass employees and affiliates who are required to read and acknowledge its content.

Please note this document provides a general construct for work performed at Cutlass. Cutlass is a rapidly growing organization that continues to flesh out its administrative processes as it strives for greater efficiency and formality of operations. Some administrative practices are more mature than others, and as all practices improve and are updated, those improvements will be reflected

in this document. This document is not meant to be all encompassing or limiting in performance of work. In the spirit of entrepreneurship, common sense and cooperation, it is expected that Cutlass, its affiliates and sponsors work together to produce high quality products using best business practices and to resolve misunderstanding with dialog where this document is incomplete. This document should be used in conjunction with other Cutlass publications, such as the Cutlass (Code of Conduct) Compliance Document to understand both the corporation's expectations and business practices.

## **2.0 Employment & Services Contracting Practices**

Cutlass primarily establishes affiliate agreements with others to develop and maintain its products. As a result, there is currently only one employee at Cutlass, its founder and owner, Steve Bull. As a result, Cutlass has not invested energy in creating a formal set of employee policies and procedures. Cutlass is committed to being compliant with all state and federal employment laws. It is also committed to fostering a work environment for its employee and affiliates that is safe, secure, and free from inappropriate behavior.

Affiliate agreements are a key success factor for Cutlass. In some cases, Cutlass will offer percentage returns on a particular product (or other compensation) in exchange for affiliate services that are key to the development of that product. This creates a significant sense of accountability to affiliates as “shared-fate” stakeholders in the development of work products. As a result, Cutlass provides regular reporting to its affiliates regarding the over-arching status of a project. Affiliates are also proactively engaged during negotiations with investors, or major “BETA” test partners/customers. Attachment 2 of this document includes a sample of the Affiliate Agreement used by Cutlass to engage the services of others.

## **3.0 Security Practices**

### ***3.1 Physical Security***

Physical security management is divided between the day-to-day operations of Cutlass and the data center supporting all Cutlass products and projects.

Cutlass established strategic partnerships with Harmonic Ranch, 1&1, Twilio, VoicePulse, Lylix, Verizon Wireless, Apple iTunes Store, Android Store, Orange wireless worldwide and Cellmania worldwide to provide database/application servers, SMS/VoIP integration and support for products in domestic and worldwide distribution. These firms were selected because their three tiers of (physical, technical, and administrative) security are compliant with National Institute for Standards and Technology protocol requirements.

Day-to-day operations occurs primarily at Cutlass headquarters at 56 Ludlow in New York City. Cutlass utilizes a password protected, multi-door lock and intercom system to prevent unauthorized access to its operations. Additional physical security is provided through off-hour alarm and canine guard services.

### ***3.2 Technology Security***

Cutlass uses the following core technology and security protocols in development and support of its products:

- Password protected access to MySQL data bases. On the web interface to the hosting site a password is required to gain administrative access to the MySQL data bases.
- Secure Shell (*SSH*) protocol for web access to application. This is a UNIX-based command interface and protocol for securely getting terminal access and transmitting data to a remote remote servers.
- Password protected SFTP aka SSH FTP protocol is used uploading files.
- PHP files accessing MySQL database use login data base name and password that are in another file to avoid as an additional security protocol when certain PHP code is shared with affiliates. This separation of duties is considered adequate for Cutlass during product development
- Affiliates are assigned unique user names and passwords that are specific to the domains or projects that might require their work or recoding. Thus affiliates are unable to access other Cutlass projects that may be located on the same server. These unique user names and passwords are destroyed when the affiliate is no longer working on that particular project.
- All passwords, including administrator passwords, are changed every six months.
- Servers are located at two distinct telephone companies. - Verizon and ATT/Southern Bell on a different network. Co-location facilities are used by Cutlass for all development and production services. These have different internet trunk lines to assure 24/7 delivery of messages with 100% redundancy.
- Telephony and other transmission of data occur using standard protocols. Cutlass presumes and research shows that the cell phone is a primary and private communication device for almost all users. Cell phones are password protected by those individuals requiring privacy and security. Cell phones and telephone have unique identification markers that facilitate Cutlass in identifying callers in automated sessions. Callers that use non-identified telephones to contact are required to enter user identification and password.

### ***3.3 Administrative Controls***

The following are several of Cutlass' administrative controls:

1. Training – Cutlass provides basic training to affiliates, business partners, and potential clients regarding the need for security and confidentiality with the use of its products. For example, EZfollowups recording could contain business-sensitive material and PreMinder may be used in ways that require compliance with HIPPA. Training for affiliates and business partners is provided informally based on the circumstances of their experience and the product. Training for clients is designed into the users' guides, developed as needed for each product.

2. Non-disclosure agreements – Advisers, sponsors, affiliates, and collaborating customers who come in contact with ideas and preliminary work products of Cutlass will be required to sign non-disclosure agreements prior to their exposure to that information.
3. Affiliate agreements – Cutlass Corporation engages others in its work through formal affiliate agreements. Each agreement is unique, though a sample agreement which includes some common conditions is shown in Appendix 3 of this document. In addition to reflecting specific work agreements, these indicate acceptance by the affiliate for working within Cutlass' administrative and ethical boundaries. These agreements are considered business sensitive and access is restricted to the principal parties.
4. Complex Passwords – All computers used by Cutlass employees and affiliates on Cutlass projects or products are required to retain password protection on the database, application library, documentation library, and any other location where sensitive data or business information is stored. A complex password is one that is at least eight characters long, case sensitive and a mix of alpha, numeric, and special characters.
5. Artifact management – All hard copy documents produced by Cutlass that contain data from one of its projects or products (such as a PreMinder report on medication compliance) are kept in a locked drawer or shred/burned when not in active use. Business-sensitive documents will be labeled as such and managed using version control and read/write access based on the Cutlass need-to-know guidelines.
6. Separation of Duties and Need-to-Know Access – Cutlass and its affiliates provide niche expertise in the development and management of products. As a result, compartmentalizing work and access to the tools necessary only to complete that work reduces Cutlass security risk. It is the responsibility of Cutlass management to ensure appropriate access to business information. This is performed on a case by case basis, considering the sensitivity of the information, work being performed, and duration of the assignment.
7. Protocols for Production Support vs. Product Development – Cutlass applies all the security, privacy, and other conduct of operations practices equally for both production support and product development. The only noteworthy exception to this is the presence of a Production Control Manager independent of development work. Cutlass uses Configuration Management practices as described in Section 5.0 of this document.

## **4.0 Other Administrative Practices**

### ***4.1 Investment Administration***

Occasionally, Cutlass will obtain investor funding to support its product development or deployment costs. All acquisitions by Cutlass are approved by the principal owner of Cutlass.

The general terms and conditions of an investor agreement is communicated to Affiliates-as-Stakeholders and an acceptable set of financial outcomes is negotiated for all. Investor opportunities are considered highly sensitive. As a result, specific investor agreements are

retained in confidence within Cutlass.

In support of full transparency, general balance sheet and income statements as well as investor financial reports are provided to both investors and Affiliates-as-Stakeholders. Note that these may be limited to a specific product under development.

#### ***4.2 Purchasing and Acquisitions***

All acquisitions by Cutlass are approved by the Principal Owner of Cutlass. Purchase requests and purchase orders are currently not used within Cutlass for material or service acquisitions.

#### ***4.3 Financial Accounting***

Cutlass maintains its financial accounts generally acceptable accounting principles and reports to state and federal officials consistent with the laws and expectations for a State of New York, Subchapter S Corporation. It retains the services of George Farley CPA for tax accounting purposes.

Cutlass is also responsible for investor reporting of financial transactions. A quarterly report is drafted for investors on a case-by-case basis.

#### ***4.3 Project Planning and Control and Other Administrative Tools***

Cutlass applies its risk-based, graded approach to the conduct of projects as well. Larger projects include the use of a trained and certified Project Management Professional.

Cutlass uses the following software: Microsoft Project 2010, Oracle Open Office, and Google as its standard suite of administrative tools.

### **5.0 Quality Practices**

#### ***5.1 Configuration Management***

Cutlass follows configuration management (CM) best practices in its software development and promulgation practices. Three IT environments are used by Cutlass: ALPHA, DEVL, and PROD. ALPHA is typically used by developers on their remote units. DEVL is a formal environment where unit testing and system integration testing is performed. PROD is reserved.

Note the following rules regarding CM at Cutlass:

- PROD code is only checked into service after a peer code review or walk through.
- DEVL tests are never run on PROD databases. Copies of PROD may be used for DEVL consistent with database refresh schedules set by Cutlass management.
- Code and other artifact naming practices will assure that PROD elements are prefixed by P- while DEVL and other elements are named D- or other, non-PROD designator.
- Note that these rules apply as appropriate for non-application based work at Cutlass. This includes maintaining corporate web pages and other elements that benefit from formal configuration management.

## ***5.2 Software Development/ Quality Assurance***

Cutlass is dedicated to a quality assurance program and continuous quality improvement in all its products and services. Cutlass performs an annual risk assessment of its technical and administrative practices as well as a formal lessons learned program after each major product release.

Cutlass uses a Plan-Do-Check-Act cycle in its development and conducts The development methodology favored by Cutlass is Rapid Prototyping where Alpha and Beta releases are brought quickly forward and then modified/re-released based on user feedback.

Finally, an important consideration for Cutlass when forming business partnerships is the presence in other organizations of a quality improvement ethic. Further, Cutlass uses ISO9000 certification as a critical data point when considering partnerships. In establishing affiliate or other agreements, Cutlass strives to contract with the best and the brightest. As a result, it uses the presence of degrees, certification, and other information when establishing these agreements.

## ***5.3 Risk Management***

Cutlass performs an annual review of its operations to improve efficiency and reduce risk. As a part of its recent work in developing PreMinder, Cutlass performed this review in October, 2011 and developed a risk mitigation plan. As a small company, Cutlass uses a graded approach to risk and integrates action plans from risk reviews into the overall project and operating plans of the company. Appendix 2 provides a detailed explanation of the risk process completed in 2011, plus any subsequent processes developed after this document is published.

## **6.0 Planning and Communications**

Cutlass performs regular brainstorming sessions with selected affiliates as a part of its strategic and tactical planning process. These sessions serve as the basis of quarterly and annual goals and objectives. Cutlass has identified expanding and documenting this process as an important quality improvement opportunity.

Cutlass uses face-to-face, email, SKYPE, and telephone for the majority of its communications with affiliates, investors, and others. Cutlass also uses internet technology such as DropBox to facilitate the development of documentation.

The majority of more formal Cutlass communications are directed in support of their projects and products. As a consequence they contain few, if any references to Cutlass itself. The majority of these are publicly available through product web sites such as:

iTunes selling AZZA - <http://itunes.apple.com/us/app/azza-v1-01/id399344175>

Verizon Wireless selling Pet-Pals - <http://pet-pals.com/>

Other Cutlass projects delivered world wide by Cellmania - <http://cellmania.com/>

Cutlass Treasurs Hunts – booking agent <http://www.dcaproductions.com/>

## Appendix 1 – Document Naming and Management Protocol

All critical documents should be stored in the Cutlass server and be included in data back up processes. In addition, employees are encouraged to use the product DropBox repositories at dropbox.com. Employees and affiliates must be invited by Cutlass to use its folders on DropBox. Employees and affiliates will have restricted access to folders on a need-to-know basis. As employee and affiliates tasks change, their access to unnecessary folders will be discontinued. The following applies to all documents produced by products of Cutlass, emphasizing the naming convention of the product (in this example - PreMinder)

Names should be brief and descriptive. Anything to get rev-ed should start Rev0. Increment as appropriate So we know who has done the latest, after the Rev0, put initials. Don't timestamp docs

example: PreMinder Project Plan V05wbh.odt

One-time use documents and artifacts should just have a descriptive name perhaps with a time context. A pdf is a one-time use document in my opinion

example: Nov PM presentation to ER.pdf

Additional Notes:

In the future we might want T- to indicate technical and C- to indicate communications and A- for administration as a document prefix.

If people want to edit/update a document, they should alert others that they are doing so and when the update might be available to avoid stepping on work. The editor should use “Save as” to save the file and attach their initials followed by a date stamp to their work.

example: PM Admin Guide v1.0 sb20111121.odf (this document edited by Steve Bull on Nov. 21, 2011)

Regarding retention requirements

Using version numbering as described above, record copies of documents will be retained in the normal course of daily operations.

## Appendix 2- Risk Assessment Methods and Results

In October 2011, Cutlass Corporation performed a risk assessment of its technical and administrative practices. The following summarizes the results of that assessment. The following table summarizes the high level criteria and considerations. Please note this is an evolving process.

### Risk Impact Categories

- Health
- Safety
- Environment
- Personal Privacy Data
- Corporate sustainability

<b>Risk Number and Description</b>	<b>Risk Vectors &amp; likelihood</b>	<b>Possible Impacts</b>	<b>Relative Score</b>
1. Disclosure of client or privacy data	Customer telephone - low Business partner - low	Threat to client well being Threat to business partner	1
2. Loss of data	Server farm crash – low Dropped call - low	Threat to client well being Threat to business partner	2
3. Loss of connectivity with client – sustained down time	Server farm crash – low Dropped call – medium/low	Threat to client well being	1
4. Theft of intellectual privacy	Affiliate - medium Business partner - low	Threat to business	3
5. Trademark or other infringement	Apple or other application store – high	Threat to business	4
6. Financial theft	Family – low Street crime - low	Threat to business	9
7. Loss of data integrity	Business partner – Unknown Poor quality - low	Threat to business partner Threat to business	7

Using a graded approach, a mitigation plan was developed as a result of this assessment based on the relative score for each risk area. Only items with scores 5 or higher were addressed in the first set of mitigation actions.

<b>Risk Number and Description</b>	<b>Mitigation Actions</b>
1. Disclosure of client or privacy data	Assure client understanding of actions they should take. Assure data separation and access control of PROD data from unauthorized affiliates or employees Work with business partners to encourage best practices are in use in all organizations
2. Loss of data	Maintain scheduled back up routine Ensure redundant systems and fail over technology Partner with certified IT service providers Pursue Cutlass-internal infrastructure
3. Loss of connectivity with client – sustained down time	Ensure redundant systems and fail over technology Partner with certified IT service providers Pursue Cutlass-internal infrastructure
4. Theft of intellectual privacy	Ensure rigorous affiliate agreements Ensure equitable pay practice Use “trade secret” method to protect predictive analytic formulas
5. Trademark or other infringement	File with USPTO for trademark and copyright protection Rapidly develop and deploy product

*Note: The public version of the risk vector analysis and mitigation plans was removed due to their extreme business sensitivity. Please contact Cutlass Corporation if you wish to examine this document.*

**Appendix 3- Agreement Templates and Samples**