Secure Communication Standard Operating Procedures and Protocols

SGR, Inc.

Revision 1.0

**Purpose and Introduction**

The purpose of this document and the SOPs, protocols, and rules herein is to ensure the safety and security of *all* members of SGR, Inc. Each member is *strongly encouraged* to consider the wellbeing, safety, and security of all other members at all times. Each member is *required* to strictly adhere to all rules, protocols, and Standard Operating Procedures within this document.

**Title and Protocols**

The title of this document shall be formally referred to as *Secure Communication Standard Operating Procedures and Protocols*. This document outlines the Standard Operating Procedure (SOP) associated with each of the six communication protocols sustained by SGR, Inc.

The aforementioned six protocols are:

1. ShitIsCasual™ Transmission Protocol (SICTP).
2. ShitIsCasual™ Reception Protocol (SICRP).
3. ShitIsCasual™ Pad Protocol (SICPP).
4. ShitGotReal™ Transmission Protocol (SGRTP).
5. ShitGotReal™ Reception Protocol (SGRRP).
6. ShitGotReal™ Pad Protocol (SGRPP).

Each of these protocols will henceforth be referred to by its five-letter acronym. The Standard Operating Procedure (SOP) associated with each of the protocols is outlined herein. The corresponding SOP shall be strictly adhered to by all members of SGR, Inc. in every usage of any of the aforementioned protocols.

**Protocol Usage Rules**

All members shall strictly adhere to the following rules regarding the usage of the protocols.

*Reception Rules*

1. If a member receives a communication that was sent via SICTP, the member shall only receive the communication according to SICRP. No other method of receiving the communication shall be used. The receiving member may elect to reject the communication.
2. If a member receives a communication that was sent via SGRTP, the member shall only receive the communication according to SGRRP. Every reasonable effort shall be made to receive the communication via SGRRP within a reasonable amount of time. If the receiving member is unable to receive the communication via SGRRP, the receiving member shall reject the communication.

*Transmission Rules*

1. If a member (sender) wishes to communicate information which if discovered by a third party could potentially cause harm to *any* other member, then the sender shall only transmit via SGRTP. If the sender is unable to employ SGRTP, then the member shall refrain from transmitting the information. However, in the case where failure to transmit the information could potentially cause harm to *any* other member and the sender is unable to employ SGRTP, then the sender may with due consideration elect to transmit the information via SICTP.
2. If a member (sender) wishes to communicate information which if discovered by a third party could *not* cause harm to *any* other member, then the sender may elect to transmit via SGRTP, SICTP, or unencrypted communication.

*Pad Creation and Sharing Rules*

1. If a pad is created or shared to be used for actual communication, it shall be done via either SICPP or SGRPP as appropriate.
2. If a pad is created or shared for system demonstration, debugging, or testing purposes, the pad shall be clearly marked and identified as such, and any usage of the pad shall not be considered to be adhering to a protocol or SOP.

**SICPP Standard Operating Procedure**

The following outlines the official SOP for using ShitIsCasual™ Pad Protocol. This protocol is used for the generation and distribution of ShitIsCasual™ communication pads.

1. At the time a pad is generated, it shall be permanently designated to a single *one-directional* channel of communication. That is, a permanent sending member and receiving member. Only a sender/receiver may generate a pad, and may only distribute this pad to the other member, such that any pad is possessed by exactly two individuals: the sender and the receiver.
2. At the time a pad is generated, it shall be given a permanent security level designation. This security level is subjective, but shall be agreed upon by both sender and receiver who will use the pad. It is recommended that the security level be designated proportional to the care taken in the pad creation and sharing process.
3. Use the official entropy generation software to create a pad of the desired size. Assign the pad a completely unique identifier code. The identifier code design is left up to the member(s) creating the pad.
4. Name the pad file according to the following convention: “SICPAD-” followed by the pad code followed by a ‘.’ followed by the extension “cpad”. (“cpad” is short for Casual Pad).
5. Distribute the pad to the other possessor via any means that does not involve a network. Distributions by USB flash drive, Compact Disk, or SD card are all acceptable examples. Do *not* distribute via WiFi, LAN, or Internet.
6. Ensure the recipient of the pad fully comprehends the purpose of the pad: the sender and the receiver of communication along with the security level.

**SGRPP Standard Operating Procedure**

The following outlines the official SOP for using ShitGotReal™ Pad Protocol. This protocol is used for the generation and distribution of ShitGotReal™ communication pads.

1. ShitGotReal™ pads have no individual security levels; all ShitGotReal™ pads use maximum security.
2. At the time a pad is generated, it shall be permanently designated to a single *one-directional* channel of communication. That is, a permanent sending member and receiving member.
3. Only the recipient shall generate a pad, and may only distribute this pad to the sender, such that any pad is possessed by exactly two individuals: the sender and the recipient. The sender may not generate a pad, but instead must obtain the pad from the recipient.
4. Generate the pad using the official software on the Secure Receiving Computer on the SGR Communication Board.
5. Assign the pad a completely unique Pad Code according to the following scheme: [Sender Last Name]-[Receiver Last Name]-[Random Unique Number Identifier]. For example: “Hershey-Umhau-3781” is a valid pad identifier code.
6. Name the pad according to the following convention: “SGRPAD-” followed by the Pad Code followed by a ‘.’ followed by the extension “rpad”. (“rpad” is short for Real Pad.) For example: “SGRPAD-Hershey-Umhau-3781.rpad” is a valid filename for a pad.
7. Save the pad to the local hard drive of the Secure Receiving Computer.
8. Insert into the Secure Receiving Computer a Dedicated Pad Transfer Device.
9. Format or otherwise wipe clean the Dedicated Pad Transfer Device.
10. Save a copy of the pad onto the Dedicated Pad Transfer Device. You may also elect to save a hash of the pad onto the device.
11. Remove the device and physically give it to the sender.
12. Sender, take the device and insert it into your Secure Transmitting Computer. Copy the pad onto the local hard drive of your Secure Transmitting Computer. If a hash is present, verify the pad using the hash.
13. Format or otherwise wipe clean the Dedicated Pad Transfer Device. If said device is a write-once technology such as a Compact Disk, either destroy it or place in a safe, secret, and secure location.
14. Send a message to the recipient via SGRTP as quickly as possible indicating the success of the pad transfer.

**SICTP Standard Operating Procedure**

**Definitions and Terms**

Dedicated Pad Transfer Device – A storage device which has been dedicated to the purpose of transferring ShitGotReal™ pads between SGR Communication Boards. A Dedicated Pad Transfer Device must never since it was bought new have been inserted into any device other than a Secure Receiving Computer or a Secure Transmitting Computer.