In light of the recent security breaches at OCRAI, and considering your unique circumstances, we have devised a method by which OCRAI employees can encrypt and decrypt text messages. In devising this particular system we had three goals in mind: simplicity, efficiency and effectiveness. We feel that our system is simple enough that any and all employees will be capable of understanding it’s implementation. We are confident that the system is efficient enough so that the encryption and decryption of messages will not take unreasonable amounts of time to complete. This system is also effective enough to keep any and all of your enemies from being capable of tampering, interfering, or infiltrating your data in any way.

The system functions in a two-step process: first, a substitution cipher to convert letters into numbers. Then, our second step consists of further encrypting the numbers by the use of modular arithmetic. As modular arithmetic is something you may not be familiar with, we will explain its operation as carefully as possible as we get to that step.

To accomplish the first step of our system, we simply need to establish some method by which the numbers 0-25 each represent one of letters in the standard alphabet. For example, a=10, b=3, c=5...etc. We suggest that you change the way that the letters are assigned on a somewhat frequent basis.

The second step of our system is to encrypt the numbers that have been established as equivalent to respective letters of the alphabet. We will do this by using modular arithmetic as mentioned above. In modular arithmetic, we can have several numbers that are equivalent to one another. We determine this equivalence by the remainder that they leave when divided by our “modulus” or key number. To ensure a successful system, we should choose our key number to be a prime number greater than 25. This will ensure that we can have an equivalence for every number from 0-25.
To demonstrate how this will work, let’s try an example: Let’s say that we would like to encode the letter z, which we have chosen to be represented by the number 15. Thus we have $z=15$, and we would like to encrypt this information further with our second step. We need to choose our key number, let’s assume in this instance that it is the prime number 373. An equivalent number to 15 will be any number that when divided by 373 will leave a remainder of 15. Thus $373+15=388$ is one such number. Or $373\times2 +15=761$. (We here realize that the possibilities for representing 15 are endless, we must only be mindful that we choose those equivalents that are within the desired length limitation). One important item to note is that in this instance the prime number 373 would represent the number 0, as would $373\times2=746$. (As both 373 and 746 leave a remainder of 0 when divided by 373).

Thus, to encrypt a given message we will perform the following: First, convert the letters into numbers using a substitution key of our choice. Second, encrypt these numbers further by replacing them with equivalent numbers that can be found by application of our “key number.” To decrypt a given message, we simply do the process in reverse. Knowing beforehand the “key number” and substitution key for the message, we will first convert the given numbers to their equivalent numbers in the set of numbers 0-25. Then we will apply our substitution key to convert each number from 0-25 into its corresponding letter.

These are the mechanisms that will drive the heart of the system. You can, if you desire, devise your own methods of how to separate letters, how to separate words-etc. For simplicity’s sake, you may choose to simply use commas for separate letters and actual spaces for spaces between words. There is no need to be overtly complicated in this endeavor, as the first two steps of encryption should be more than sufficient to keep your information safe.

We do insist that you frequently change your “key number” – this will keep your enemies from attempting to cycle through all prime numbers in an attempt to discover your key number. This will make your encryption near impenetrable, even by the most powerful of computer decryption methods. It is important to note that the bigger your “key number,” the harder it will become for your information to be
deciphered. If, by some stroke of luck, your enemies manage to obtain or guess your key number, they will still only have a list consisting of the numbers 0-25, which is meaningless without the key used for your substitution cipher.

It is also important to note that your enemies will have a hard time trying to send false communication using your encryption method – as they will not know the keys used, and may send a message that appears to be from your company, but will fail to be deciphered when you apply your actual keys. You will decrypt a bunch of nonsense, and can thus realize that the communication is certainly not from someone in your company. (You realize the improbability of your enemies guessing both of your keys accurately).

We here at the IMC feel very strongly that the encryption method we have outlined will efficiently meet your security needs. The system is easy to use, easy to maintain, and requires very little knowledge of mathematical or computer programming knowledge. Employees need simply be capable of performing division, which can be accomplished on any basic calculator. The system is also very effective and capable when it comes to keeping your information encrypted and safe. The encryption and decryption processes are also relatively quick to perform on messages of the considered size. We are confident that our system meets the goals of simplicity, efficiency and effectiveness that we felt was necessary for your particular situation, and we stand by the fact that this system will more than adequately meet your specific needs.