PREAMBLE

We, as the information owners and stewards of the world, declare that the current way computers define and manage our information is incorrect and unacceptable. We will no longer be ignored, blamed, bullied, or discounted by vendors in the computing industry. Your current computing capabilities, which haven't fundamentally changed in 50 years, will no longer be acceptable. The following "Bill of Rights" defines what we expect to be provided. The "Declaration of Independence" is what we are not going to put up with any longer.

Information Owner's Bill of Rights

- We are the ones responsible for our information, not IT, the CIO, the CISO, or anyone else.
- As such, we are the best people to specify the information and its required lifecycles. We demand a say in how these systems are specified, selected, and operated.

Information

- Our information is the most valuable part of our computer system and therefore, should be treated with the attention and respect it deserves.
- The unit of information we work with, think about, talk about, communicate with, etc., must be understood by our computing systems.
- Our unit of information is a collection of files, metadata, audit records, emails, people, etc., that, as a set, is meaningful to the organization.
- When anyone attempts to locate our information, they always get the most recent, valid, approved version (Single Source of Truth).
- We have the right to know where all other copies of our data are also stored.

Processes

- Processes that operate on our information must be simple and safe.
- No operation on our information should put its existence or integrity at risk.
- We expect automatic and accurate records be kept of all operations on our information.
- Process "Best Practices" may need to be tailored to our specific circumstances and requirements.

Protection

- We expect the system to protect the integrity of our information.
- Bad things happen. We expect the system to do everything it can to ensure our information is recoverable from any disaster.
- Our information will be continually monitored and protected from unauthorized, accidental, malicious, or unintentional modifications.
- Should someone manage to perform an unauthorized modification, the correct information should be put back automatically and immediately.
- We must be able to safely expose our information to the right people at the right time without fear it will be compromised or corrupted.

- We must be able to quickly locate the correct information by many different means and criteria, no matter how it was initially stored.

Costs

- Any information system must be affordable for any information owner at their organizational level.
- The system must have a pricing model that can be understood, predicted, and budgeted, regardless of any external services that are in use.
- Any license model will not inhibit the use of our information by the correct people as part of its lifecycle requirements.

Future

- The system must be flexible enough to respond to our ever-changing business, organizational, legal, and regulatory requirements.
- While we can never underestimate the cleverness of cybercriminals, we expect our system to have a long-term plan to stay ahead of these cybercriminals who are attempting to attack our businesses.
- As part of that long-term plan, we expect the system to continue to incorporate new security and protections without making the information processing operations more difficult or restrictive.

Declaration of Independence

We, as the information owners and stewards, declare our independence from the following items, tasks, and issues that make our jobs so difficult. These are the things we no longer want to deal with, be exposed to, put up with, learn about, make decisions about, or have to pay someone to do for us in order to keep your products running.

- **Technology Independence:** All the complex technology that is required to meet our demands as outlined in the "Bill of Rights" needs to be hidden. We don't want to see it, be exposed to it, have to learn about it, make decisions about it, run some sort of GUI with it, or pay someone to do all that for us. It should be preconfigured, automated, and hidden. We don't even want to be exposed to the terminology of all that technology. We have businesses to run.

- **IT Independence:** Many of us either don't have access to professional IT services, the services are limited and/or expensive, or the available staff is overworked and overloaded making it very difficult to gain any of their attention. We view IT as an unreliable component of the systems that make our jobs more difficult. Don't you think it is a bit ironic that computers have automated just about every process in the world except one? Running computers! We feel it is unacceptable to have to hire highly trained, expensive, and scarce manual labor to setup and run computer systems for us.

- **Integration Independence:** We expect that if we select a system to manage our information that the system is a "complete solution". We don't want to have to find out later that we need something else like a dedicated database server or some additional expensive software and have to pay someone to do that integration in order to get the system working. We think it is wrong to have to force every computer owner or organization to identify, select, install, configure, test, run, monitor, and repair all the pieces of the technology. That is a huge waste of our time and money. You are the ones best positioned to do all this integration. Do that BEFORE we get the product and make sure it works. We know it is complex but passing off dealing with that kind of complexity to every IT operation on the planet seems a bit less than optimal to us.

- **Information Entropy Independence**: Entropy is the "disorderliness" or randomness that is constantly at work degrading the integrity of our information. We expect the system to ensure the integrity of our information is protected at all times.

- **Perfect User Independence:** Today's technology requires everyone to do everything perfectly. One slip up can result in the loss of a tremendous amount of work. No matter how stressed out, hurried, overworked, interrupted, clueless, forgetful, clumsy, inattentive, untrained, or oblivious we are, make sure we (or anyone else for that matter) can't destroy our information.

- **Perfect Internet Connection Independence:** The people that rely and use the information we manage need that information accessible at all times. Many of us have policies or regulatory reasons that any data we save must be available on-site. Some of us are subject to surprise audits that can have dire consequences to our organizations should the information become

unavailable if the internet connection is down, restricted or overloaded with zoom calls. Your system can use the internet and probably has to but we don't want to lose access to our information due to loss of connection.

- **Cybercriminal Independence:** As obvious as it sounds, please make things more difficult for cybercriminals and less difficult for us and our users. Put in enough detections, configurations, information copies, automated processes or whatever you need to do so we are not just one errant mouse click away from information and/or financial disaster.

- **Ridiculous Decision Independence:** Don't force us to answer questions that we are not qualified to answer. Especially don't ask us questions that you should have already answered. Don't make us save something, remember something, keep something, have something, or do something that if we don't, the very recovery of all of our information is then impossible. Don't ask us questions like how much of our teams work are we happy to throw away because backup is so inefficient and broken. We are going to always say zero minutes so respond accordingly. We don't want to have to set your gonkular phase angle (whatever that is). You do it.

- **Data Hostage Independence:** There should be no situations where we cannot at least access our information. People's location, your pricing model, system failure, your company closes, or anything else, we'd better be able to recover all of our information we entrusted you with. We simply won't use a service where the risk to the recovery of our information is too high.