Author: **Mr. Quan Nguyen**

How do You Customize a Good BYOD (Bring Your Own Device) Policy?

As BYOD (Bring Your Own Device) becomes a necessity rather than an option, attitudes about employee mobility and the organization's movement will continue to evolve. Your BYOD policy needs to be better evaluated: Your policy must be a living, breathing document for your employees and your organization.

As an organization, you will need to have a clear understanding as to how you can manage this daunting task with clearly-defined and quantifiable policies and procedures.

What does a BYOD device policy need to contain, and what should it say?

1. Your organization needs have an understanding and clarify exactly what data is being used for business and what is personal. This is easier said than done, so you will need to be meticulous with this endeavor.

2. You need to have two "dirty little words:" Policies and Procedures! No one likes policies and procedures, but they are necessary to protect both parties. Within this document, you need to have a complete and thorough definition as to what content is business data. Once again, you should know that email and business-related documents are the norms. What about photographs, phone numbers, texts and other data? You cannot make assumptions about what's business and what's personal.

3. As a natural progression for BYOD, organizations are "heavy" on the company's rights to access devices. However, there needs to be a balance between company rights and employee rights. This is something that you will need to discuss thoroughly with your legal and human resources teams.

4. The policies and procedures need to clearly state how your organization will need to protect your data as well as what platforms will be supported and how, what service levels a user should expect, what the user's own responsibilities and risks are, who qualifies, and your compliance requirements. You will need to work with IT on this because IT provides guidelines for the users.

5. The message to your employees is this: **Read** every policy carefully and make sure you understand it. Ask questions!

6. Incorporate a "trust but verify" approach for your users. Carry out inspections, review the data regularly, examine the devices and regularly, assess the process relating to the users, the data at rest, the data in transit, the data being used, and the entire audit trail.