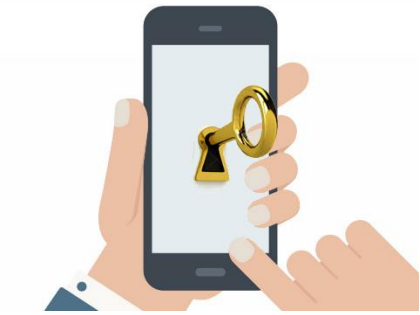
Intellect Partners - Our Security, Customer Focus, and Unique Approach

Intellect Partners

Table Of Contents



Why Digital Trust Matters

Whenever a client decides to purchase an organization's digital product, they're communicating trust in that business. According to this viewpoint, each web-based purchase is a demonstration of digital trust. Then again, if research, related knowledge, or brand reputation leads somebody to think that a digital business is not reliable, they'll go somewhere else. The more digital trust an organization can hold, the more clients it will be able to draw in. Recent research has shown that a 5% increment in client dependability can support lifetime client value by as much as 76%.

Individual purchasing choices straightforwardly correspond to digital trust. Three out of four US consumers say they're probably not going to at any point buy from a digital brand they don't have trust in, and 47% of Americans report that they'd for all time quit utilizing an organization's administration assuming they discovered that a breach or abuse of their information had occurred in the organization.

On a national and, even worldwide scale, digital trust upholds and empowers financial development. As the world economy becomes progressively reliant upon always-on connectivity, information trade, and technological advancement, digital trust is progressively turning into an essential piece of business.

As the digital business ecosystem keeps on growing, an association's capacity to develop digital trust will turn out to be progressively imperative to its prosperity. This is the reason, as per expectations made by IDC Research, above 33% of associations will have supplanted Net Promoter

Scores and comparable measurements with digital trust files by 2025. Throughout the following, not many years, clients and markets will request a bound together way to deal with estimating trust and will start to utilize quantitative measurements to survey things like security, protection, consistency, and client experience.

The downstream effect of this mounting accentuation on digital trust will be a more grounded organizational focus on privacy and cybersecurity. Progressively, cyber risk alleviation and information security will be considered fundamental guarantors of client experience. To keep away from excessive - and possibly decimating - risks in an unstable and unsure future that will request business agility every step of the way, decision-makers should join network safety procedures into the core of each digital change drive that their organizations embrace.

Our Commitment to Data Protection

It is our obligation to safeguard the personal information that we collect. Our reputation relies upon it. We know our clients, employees, and other individuals care about their privacy, and we are committed to acquiring and keeping up with their trust. At the point when we gather, use, keep up with, or share individual data, we focus on keeping it safe and involving it for the reasons portrayed in our privacy policies and notices. We work consistently with security regulations and regard the privacy rights of individuals. We require our business colleagues with access to our information to do likewise. We only offer individual data to those that are approved to get it.

We safeguard individual data by keeping up with data security programs sensibly and suitably intended to address security risks and safeguard the privacy, security, confidentiality, integrity, and accessibility of the data. Assuming we become mindful of a breach of information in our organization or a breach including any of our information that is in the ownership of our suppliers or business partners, we will make a quick move to appropriately notify and safeguard the individuals who are impacted. We comprehend that our reputation and achievement rely upon keeping up with entrusting information protection and security.

Why does Our ISO/IEC 27001:2013 Certification Matter?

ISO 27001:2013 certification is something imperative to search for in any cybersecurity partner since it shows an association-wide commitment to security. Working with such a partner can help your own organization's security. Here and there the best method for managing information security risk is to either eliminate it or outsource it to a third party.

For instance, by picking an identity and access management (IAM) platform to deal with your client passwords, you offload some gamble by not putting away sensitive information on your servers. Also, utilizing an ISO 27001-confirmed IAM supplier (as Auth0 has done starting around 2018) sends a message to your clients and accomplices that your information is secure.

ISO 27001 is likewise the foundation of a developing international agreement about information security best practices. Australia based its government's Digital Security Policy on ISO 27001. Similarly, ISO 27001 can

give direction on the most proficient standards to satisfy the guidelines of different information protection regulations, for example, the GDPR, which regularly directs organizations to it to act as an example of universal prescribed procedures. So on the off chance that you submit to ISO 27001's suggestions, you're on right track for lawful consistency, also further developed information security.

Customer Focus

Our clients are the reason that we exist. We mean to meet and even surpass their needs and expectations to make them effective. We will even attempt to anticipate their requirements and present solutions they've not seen before in the soul of true partnership. Our prosperity relies on our clients' prosperity. Client center is the establishment for client loyalty since it is our guarantee to our clients to put them first. Likewise, as indicated by some new surveys generally 50% of clients say they would change to a competitor after only one bad experience. Also, that number leaps to 80 percent on account of more than one terrible experience. Turning into a client centered association is significant for assisting us with guaranteeing that clients leave the experience having a decent outlook on our image. That is on the grounds that it expects us to hold them as the directing power behind all that we do.

In any case, turning into a client centered organization doesn't mean we are suddenly an ideal business that never makes mistakes. That sort of outlook isn't useful or honest. Rather, client focus is significant for building client

connections that are more human. This includes learning from our clients and utilizing those significant experiences to improve.

Process Approach

To follow through on our obligation to add up to client focus, we continually work on our internal processes to boost their adequacy and proficiency. We perceive that it takes incalculable individual exercises to deliver our work products and services and that the process approach integrates them all. Our business is a process that transforms a few information inputs (client prerequisites, assets, talented employees, and so on) into a result that addresses our client's issues. Inside our business are a few key processes that make everything work. Our processes are reliant upon each other and individually need consistent consideration and improvement. We are continually moving ourselves to refine and change how we get things done to decrease the time it takes to finish a work product with the least error. Whenever mistakes do happen, we use them as any open doors to learn and get to the next level. We are forever discontent with how things are functioning now and endeavor to raise our game consistently.

Risk-based ThinkingProcessValue

Looking forward to guessing what could happen is the reason we utilize risk-based thinking throughout our organization. At a few places in our processes we deliberately pause and pose two testing questions:

"What could turn out badly?"

"Is there a method for improving this more?"

This viewpoint of continually looking for risks and going with opportunities drives us to action which we cautiously figure out how to guarantee ideal implementation and effective outcomes. This provides us with a demeanor of being proactive to make the most of every available opportunity to improve.

What is Product Security?

In simple words, product security is the work we do to incorporate security into the products we make. It is a customized security system that encompasses an organization’s people, processes, tools, and preparation to

ensure work products are being created and made given security. Like corporate data security, it commonly comprises different stages intended to uncover or identify product vulnerabilities, safeguard/protect the product through exercises like vulnerabilities remediation and hardening, respond to product cybersecurity occurrences, as well as continuously monitor and upgrade a product's security.

Product security in Intellect Partners

Intellect Partners has a corporate Product and Solution Security Program pointed toward reinforcing the cybersecurity of the products and solutions created across all over the organization. The areas of focus incorporate processes and tools to help vulnerability the executives of our products and solutions, design standards for security products and solution definition, and the adoption of secure design standards and secure coding practices in product improvement. A portion of the key program exercises include:

- Educating our engineers on secure standards practices.
- Scanning of items for security vulnerabilities, both while being developed and consistently after completion.
- Utilization of secure OS hardening for Intellect Partners' products.
- Expansion of explicit security highlights and controls given product/solution use models.
- Processes for rapid reaction to critical cybersecurity issues.
- Nonstop monitoring and improvement of products security practice viability.
- Secure Communications as a component of Product Security.

Protection for Intellectual Property and Safeguard Proprietary and Confidential Information

Securing and protecting the Company's Intellectual Property and defending restrictive and confidential information is basic to the prosperity of our organization. As a technology organization, intellectual property and confidential data are among our most significant resources and incorporate our brands, trademarks, know-how, inventions, patents, and other copyrighted materials, trade secrets, strategies, computer programs, and media properties, including websites and applications. We safeguard our intellectual property and confidential data and guard against their unapproved use or dissemination. We additionally regard the intellectual property rights and confidential data of others and perceive that doing so is essential to keeping up with our business and reputation. By and large, safeguarding intellectual property and proprietary and confidential data, whether it is our own or has a place with our business partners, defends our thoughts and keeps up with our reputation as a dependable partner.