E-Privacy:
A Policy Approach to Building Trust and Confidence
In E-Business

Contents

Executive Summary

1.1

The unprecedented global growth of the Internet, the promise of E-Business, and the emergence of mobile business have, and continue to have, a profound affect upon the way organisations operate. The so-called new economy, that leverages the benefits of technological convergence and new business models, offers unparalleled advantages for an immense variety of service providers and their customers in the cyber marketplace. Providers see significant economies in operating in an E-Business environment that has global reach, with the prospects of cost reductions being passed on to the customer. Similarly, for online consumers, the Internet offers infinitely expanded buyer information and a range of choices that are daunting to comprehend.

1.2

However, in spite of these apparent benefits the transition to the E-Economy has not been without problems. For many organisations there is continuing uncertainty over which operating model to adopt, and the rather intimidating lessons of some high profile failures. The global E-Business environment will continue to pose difficult and far-reaching management challenges to leaders of online businesses.Some of these challenges are already evident and have a profound effect upon the "ways of doing business". Among them, and of paramount importance, is the issue of "How E-Business can maximise its value to consumers and simultaneously retain their trust and confidence?" Building consumer trust and confidencerequires thoughtful analysis of the nature of the relationship between buyers and sellers. Not only are consumers concerned about sellers offering quality products and services, they are also concerned about their ability to exercise control over the use of their personal data. This is an issue that relates to an organisation's ability to respect and protect the personal data entrusted to it by consumers. In the E-Business environment, protection of online consumers' E-Privacy is a critical management responsibility. In any E-Business initiative, that duty has increasingly become a key determinant of business success.

1.3

The protection of personal data privacy is a corporate imperative worthy of the attention of the CEO. This does not mean that the responsibility rests solely with the CEO, but that a measured response to personal data privacy needs to be a top-driven.
In the USA the CEO may be assisted by a Chief Privacy Officer, a relative newcomer to corporate ranks. The consequence of this development is evident in management thinking and commitment to best privacy practices.

1.4

In the context of E-Business, E-Privacy has to be established as a core value that connects organisational culture with the best interests of the consumer. The value of E-Privacy can be viewed as an important indicator of business success. Worldwide, many high profile business failures are attributable to the lack of recognition accorded E-Privacy, and the lack of commitment to it as a consumer issue. The consequences of this oversight can

lead to an erosion of consumer loyalty, negative publicity, and the loss of potential business. Such effects may directly and adversely affect stock price and market share.

1.5
Not the least of these consequences though is the risk of litigation. If the early experience of the USA is any guide then there is likely to be growing sensitivity in Hong Kong around the rights of the individual insofar as their personal data are concerned. If these rights are violated then it is reasonable to anticipate that individuals will seek reparation for an alleged infringement.

E-Privacy is also a critical management consideration in evaluating and implementing E-Business initiatives, plans and proposals. Effective E-Privacy planning and implementation requires the enterprise to adopt a systematic approach. Activities in the implementation cycle involve four components:

- E-Privacy Drivers
- E-Privacy Strategic Planning and Privacy Impact Assessment
- The Implementation of E-Privacy Strategies
- The Pursuit of Excellence in E-Privacy.

1.6
These components are the foundation to building an E-Privacy Policy framework for E-Business. The effectiveness of E-Privacy Policy needs to be evaluated against the following criteria. The extent to which it reflects and reinforces a commitment to E-Privacy as a core value.

- The extent to which it upholds the concept of informed choice and consent regarding the purposes for which a customer's personal data may be collected and use.

- In the event of an alleged infringement, the provision of a mechanism that offers online customers an effective and efficient redress procedure.

- Accountability and transparency: saying what you will do, and doing what you say in terms of the protection of personal data entrusted to online business providers. In essence, the compliance measures adopted.

1.7
Having laid claim to the CEO's time, it is reasonable to ask what the pay-off from this investment in E-Privacy is likely to be? One answer to that question is that, as some commentators have observed, it is not whether an organisation can afford to adopt an E-Privacy Policy, and related practices, but whether it can afford not to do so. Simply put, the choice is no choice. There is a clear articulation of the pay-off from E-Privacy both in terms of competitive need, and the competitive advantage to be derived. The latter range from the bottom line, to building trust and confidence, to the long-term rewards of consumer loyalty.

About this handbook

2.1
This handbook is aimed at online business providers, especially those that operate websites that collect personal data. The contents are of particular value to those members of the E-Business community that are not IT specialists, but have organisational responsibility for ensuring personal data protection. The argument being that what you don't know may harm you.

The objectives are twofold.

- To establish the case for the formulation and dissemination of an E-Privacy Policy by those Hong Kong providers that collect and use personal data.

- To offer a framework that will enable providers to develop and formulate an E-Privacy Policy that will add value to their involvement in E-Business.

2.2
The policy framework presented in this handbook is specifically designed to facilitate E-Privacy in relation to personal data. It does not amount to a Code of Practice, though the Office

Background

3.1
In the HKSAR the concept of personal privacy is generally appreciated, if not always well understood. The PCO is responsible for upholding the Personal Data (Privacy) Ordinance ("the Ordinance") which concentrates on one aspect of privacy, personal data privacy. In this capacity the PCO has adopted the principle that the legal provisions of the Ordinance are applicable both online and offline. This means that those provisions, and related Data Protection Principles ("DPP" - please refer to Annex), should be complied with by providers operating in the E-Business environment. The DPP enshrine what have become the mainstays of best privacy practice, and form the backbone of legislation in an increasing number of jurisdictions. Essentially they establish the principles to be applied to the collection, accuracy, use, security and access to personal data. These principles have proved invaluable in the real world, and the PCO are committed to applying them to the management of personal data in cyberspace.

3.2
The DPP confer the following rights upon individuals.

- **The Right to be Informed of Use**
  - This right to be informed of the purposes for which an individual's personal data are to be used and the classes of persons to whom that personal data may be transferred.

- **The Right to Fair and Lawful Collection**
  - The individual's right to have personal data collected by means that are fair and lawful and for purposes that are directly related to the functions and activities of the body collecting the data.

- **The Right to Give only Necessary Data**
  - The right to give no more personal data than are necessary for the purposes for which the data are collected.

- **The Right to Consent to a Change of Use**
  - The right to be asked for consent before an individual's personal data are used for purposes other than the purposes for which they were collected, or directly related purposes.

- **The Right to Accuracy and Security**
  - The right to expect that personal data are kept accurate, up-to-date, secure and for no longer than necessary.

- **The Right to Transparency**
  - The right to ask a data user (a data user is any party that controls the collection, holding, processing or use of personal information) to disclose its personal data policies and practices, the kind of personal data held, and the main purposes for which they are used.

- **The Right of Access to Personal Data**
  - The right to obtain confirmation, and request for a copy of personal data held by a data user. The data user should comply with that request within 40 days.

- **The Right to Request Correction of Personal Data**
  - The right of the individual to request for correction of inaccurate personal data within 40 days of when the request is made.

3.3

The PCO has been monitoring developments in E-Business notably since the government announced its policy of making Hong Kong a centre of excellence in this respect. Through its network of contacts in the international privacy community, consultation with government departments and agencies, and its involvement with business and the community, the PCO has been able to identify E-Privacy risks and related personal data issues. These issues must be confronted if trust and confidence are to prevail in the provider-consumer relationship. Current wisdom suggests that until the hallmarks of trust and confidence are reflected in community perceptions, E-Business will be impeded in the realisation of its full potential.

E – Privacy Principles

4.1
The operational experience of the PCO, and the findings of research commissioned by it, indicate that there is a very real need for E-Business providers to devise rigorous E-Privacy standards, and associated best practices in personal data management if E-Business is to flourish in Hong Kong.

4.2
In promoting that objective the PCO operates on the basis of a number of principles.

- E-privacy personal data practices should operate on the principle that what is illegal offline is illegal online. Applying this fundamental rule means that providers must ensure that online and offline personal data privacy policies are dealt with in a consistent manner.

- An effective E-Privacy Policy requires the provider to inform consumers of the commitment made to the protection of their personal data, and honour the responsibility that commitment places upon management. In essence that means providers should inform customers about what they are going to do to protect their personal data, and then do what they say they will do.

- Providers should instill the virtues of E-Privacy in their staff by providing effective training. The outcome of a programme of planned human resource development should be to establish E-Privacy as a core value of the provider's organisational culture that is reflected in the attitudes and behaviour of staff.

- The formulation of an E-Privacy Policy needs to be preceded by an investigation that maps perceptions towards the central issue of trust and confidence. Where any gap in expectations exists between the perceptions of providers and customers towards the capabilities of their systems, this perceptual gap should be addressed by the provider. Insofar as trust and confidence are concerned, the perception is the reality. It is the customer's reality that providers need to clearly understand if they are to influence their perceptions and gain broad-based acceptance from them.

4.3
It is suggested in this handbook that a methodical approach to implementing E-Privacy should be based on an effective model. Before taking a closer look at the model it is as well to address the issue of why E-Privacy matters.

What is the Value of E–Privacy Policy

5.1
An E-privacy Policy may be regarded as a way of differentiating competing providers. The value of formulating, adopting and demonstrating exemplary E-Privacy practices lies in the rewards it yields. Not the least of these is the relationship that continues to exist between buyers and sellers over the long-term. The growth pattern of successful organisations is testimony to the view that there is no business like old business and anything that puts old business at risk is bad
for business.

5.2
The importance of this assertion can perhaps best be illustrated by looking at one of the most distinguishing features of E-Business; its lack of obvious physical presence. One of the contemporary cliches is that the Internet is everywhere, yet nowhere. The consequence of not having a 'bricks and mortar' identity gives rise to concern, notably when things go wrong. In the physical world a concerted attempt can be made to right any injustices. In the cyber world righting any wrongs can be a lot more problematic, if not near impossible. Direct experience of this, or the perception that something untoward may occur, is sufficient justification to reject online transactions as a means of consumption. Such a mentality poses a major obstacle in attempts to unlock the consumer power of the Internet.

5.3
Against this background the best way to answer the question posed is to look at the consequences of not being proactive in developing an E-Privacy Policy. The risks are considerable.

- **Damage to the Bottom Line**

If E-Business is conducted in a manner that pays scant regard to the privacy needs of the consumer, or in any way deludes the consumer, then the reaction from the marketplace will be swift. Consumer blacklisting or boycotting of providers is serious enough, but is made more so by the speed with which bad news travels over the Internet. It is likely that infringements of personal data privacy will have an adverse and almost immediate impact upon the provider's bottom line. If this were not sufficient cause for concern, then the loss to potential business should convince the most sceptical.

- **Potential Damage to Customer Loyalty**

Consumers can be very unforgiving of the mis-management of their personal data. They express that dissatisfaction by voting with their money and electing not to spend, or to spend offline. Having worked and invested to build customer loyalty and brand equity it is prudent to enhance those assets by adopting an E-Privacy Policy that protects the personal data of consumers.

• **Expanded Legal Framework and Regulation**
National laws on privacy, directives issued by powerful trading blocs such as the European Union, international conventions and codes of practice pertaining to the management of personal data in specific contexts e.g. medical data, all indicate that nationally and internationally, governments are taking strong measures to protect personal data privacy. The complexity, diversity and popularity of these laws suggest that a priority has been attached to privacy as an item of public policy. That policy demands industry leadership and self-regulation initiatives that communicate the importance attached to personal data privacy.

• **The Risk of Litigation**
The consequence of non-compliance with privacy laws means that providers run an increased risk of litigation. That is certainly the case in the USA where courts have ruled in favour of the plaintiff and required defendants to make financial restitution for violating privacy rights. It is likely that early precedents will give rise to growing consumer awareness, and more litigation. In implementing appropriate E-Privacy policies, Hong Kong providers are more likely to remain on the right side of the law.

• **Unfavourable Publicity**
No responsible provider wants to invite a public relations disaster because the media, or an Internet watchdog, has identified and publicised the mis-management of personal data on their site. Negative publicity can seriously damage the image and reputation of a provider and erode business prospects.

5.4
Any one of these reasons makes a good case for implementing an E-Privacy Policy; collectively, they make a very convincing case. Given the tendency for providers to collect more personal data, rather than less, it is unsurprising that consumers are increasingly cautious about releasing potentially sensitive information. First of all the Internet is an inherently insecure medium. A transmission on the Internet is potentially an open broadcast to the cyber world. Any sense of insecurity this may generate is accentuated by concerns over the access and use of personal data for unprescribed or unlawful purposes.

5.5
It is considerations such as these that are fostering a desire on the part of online users to retake control of their personal data. This means that the individual will decide whether to withhold or release personal data, and the basis upon which that decision will be made. Clearly this highlights the significance attached to the concept of informed choice which enables consumers to be selective in the disclosure of their personal data.

5.6
The reservations expressed by potential consumers towards Internet based transactions is, in part, a direct reaction to the belief that trust and confidence are not yet the hallmarks of E-Business. One of the critical factors in determining the success of an E-Privacy Policy must be the extent to which trust and confidence are associated with the operations of any single provider.

5.7
A longer-term benefit to be derived from the trust and confidence issue is that exemplary E-Privacy practices may well be instrumental in converting offline consumers to online consumers. If providers can convincingly demonstrate that privacy

concerns around personal data and the integrity of financial transactions are unfounded then this may facilitate a change in consumer habits thereby eroding the percentage of Internet users that currently reject online services.

E- Privacy: A Policy Framework

6.1
The framework offered is an adaptation of a generic planning model in that it links the sequential activities of analysis, planning, implementation and control. This cycle, depicted in the figure below, should be dynamic in responding to changes, if not capable of anticipating them. System development, trouble-shooting and upgrades should ensure that the bar is raised on performance criteria and new challenges identified and addressed.

So what does the E-Privacy Policy framework look like?

A Policy Framework

STAGE 1:

E-Privacy Drivers

- Establish an E-Privacy Culture
- Business Core Values
- E-Privacy Policy Statement

STAGE 2:

E-Privacy Strategic Planning and Privacy Impact Assessment (PIA)

- Formulate Big Picture Strategies
- Investigation and Analysis of the Business Environment
- Privacy Impact Assessment to Evaluate Risks & Challenges

STAGE 3:

Implementation of E –Privacy of E –Privacy Strategies

- Detailed Operational Strategies and Tactics
- Application of Privacy Enhancing Technologies (PET)
- Compliance and Audit

STAGE 4:

The Pursuit of Excellence in E- Privacy

- Manage E-Privacy Risks
- Enhance Compliance
- Commit to Continuous Improvement

Stage 1 E –Privacy Drivers

This initial step in the cycle requires the provider to think carefully about what the future will look like in any given business domain. For example, currently there is considerable interest in migrating the success of conventional 'bricks and mortar' operations to an E-Business format. There have been spectacular success stories in this process but many more failures. This suggests that the transfer to a new modus operandi is a complex process or that, as some observers note, the 'whole E-Business thing' has been blown out of proportion. That is, for many customers, E-Business is something that is simply ahead of its time. Certainly the evidence is that there have been difficulties in the diffusion and adoption process and Hong Kong is no exception to this.

The present state of E-Business suggests
that some providers have better conceptualised or mapped an accurate picture of the future. This has been matched with the ability to implement strategic initiatives that seek to secure that vision of the future. However, clear thinking alone is not enough; it must be matched by reasoned analysis and judgements that are relevant to the individual provider's business domain. So, any E-Privacy Policy must be preceded by reconnaissance to ascertain what is tenable, in terms of the future, for any particular provider; the contention being that E-Privacy should be a constituent element of that vision.

If this is accepted then E-Privacy needs to become a core value that influences behaviour in the workplace. A commitment to creating this value means that all planning and implementation activity must be aligned with the vision of the future. This can be seen in the following examples. to become a core value that influences behaviour in the workplace. A commitment to creating this value means that all planning and implementation activity must be aligned with the vision of the future. This can be seen in the following examples.

- **E-Privacy Culture - Creating the Value**

Organisational cultures take their cues both from the prevailing values and customs evident within the society in which business is conducted, and from the leadership of the organisation. Frequently, change in the 'ways of doing things' is met with resistance. The lessons of the past offer insights into what may happen in the future with E-Privacy. The initial ideas of thinkers on social issues such as consumerism and the environment were often regarded with scepticism. However, some entrepreneurs took a more enlightened approach by looking at these developments not as a threat, but as an opportunity for the business. That is the way in which E-Privacy should be regarded. A concept whose time has come and one that presents the provider with a new opportunity and basis upon which to compete.

The future-oriented provider should regard E-Privacy as a 'new' value. The creation of that value necessitates the support and involvement of top management. However, this leadership should go beyond the trappings of E-Privacy if the initiative is to be credible. If that is the case then a provider will benefit by creating a favourable perception towards E-Privacy as a corporate value both with internal and external customers. The challenge then is to match the expectation created in the market place. This requires a disciplined approach to the implementation of operational strategies. The danger, of course, is that

that the provider may over-promise and under-deliver which is likely to be counter-productive. Expectations should be appropriately pitched and managed.

Creating the E-Privacy value, and sustaining it, will become part of the benchmark of excellence that consumers expect of leading providers. More significantly, commitment to the maintenance of this value will result in a win-win outcome for providers and customers alike.

Though essential, creating the value may seem a rather obscure process. To try and make it more tangible it is useful to move to the micro level and look at an E-Privacy Policy Statement that encompasses the value and key features of online personal data privacy.

- **E-Privacy Policy Statement (E-PPS)**

Good E-Privacy must respect E-Privacy principles in the conduct of all aspects of online and offline transactions. This means that E-Privacy values need to be apparent in the provider's on-screen E-Privacy Policy Statement ("E-PPS"). An E-PPS is a requirement of the Ordinance where a provider collects information online from individuals, that enables those individuals to be identified. This is most likely to arise in connection with online registration or service sign-up. However, such information may also be collected through other means such as the use of cookies.

7.4

It has been said that if you can't measure it, you can't manage it. The effectiveness of any particular E-Privacy Policy statement must be measured against its ability to deliver on four key dimensions:

- **Respect for the Provisions of the Ordinance**

Providers need to create the value for E-Privacy so that it becomes one of the distinguishing features of the provider's organisational culture.

- **Accountability**

Procedures should be put in place that will ensure operational compliance on a day-to day basis. This implies the appointment by the provider of appropriately qualified person(s) whose job description addresses this responsibility.

- **Informed Consent**

The right of the customer to exercise control over the collection and use of their personal data by a provider. This can only be achieved if the provider accepts the principle of informed choice and consent.

- **Customer Redress Mechanism**

Providers should ensure that, in the event of a customer grievance, there is an effective online redress mechanism that is user-friendly.

7.5

In summary, E-Privacy Policy should seek to eliminate the possibility of unlawful and unauthorised access and use of personal data. The ultimate goal is zero tolerance.

Stage 2: E –Privacy Strategic Planning and privacy Impact Assessment

8.1
The formulation of specific functional or process strategies forms a central part of Stage 2 of the E-Privacy Policy framework. These strategies need to be tailored to the specific needs of the provider, and the market segments targeted. This will reflect in systems architecture design, the service mix, value and supply chain management, target customer needs etc. Customised strategies should be anchored to the provider's E-Privacy drivers and the direction set in
Stage 1 of the process.

8.2
The fulfillment of the provider's vision, and related privacy objectives, will make the following type of demands upon the provider.

- Irrespective of approach, the provider will need to put in place a strategic planning process that links the key activities of analysis, planning, implementation and control.

- The planning process should be preceded by a situational analysis of the strengths and weaknesses of the provider in relation to the opportunities and threats in the E-Business environment. The purpose of this exercise is to identify, evaluate, select and prioritize tenable opportunities that are attractive given prescribed performance criteria. The preferred options will invariably generate organisational imperatives and key results areas ("KRA").

- An output of the planning process should be the formulation of specific functional or process objectives, and related strategies, that are consistent with corporate objectives and E-Privacy goals.

- The next task is to break the strategy down into manageable action plans that will identify particular responsibilities and targets for individuals or teams to attain. It may also indicate the tactical approach to be deployed in the short-term.

- The execution of action plans and strategies needs to be policed by a rigorous compliance regimen. This should establish operational performance protocols that address network attacks, counter-measures to be taken, damage control procedures, performance pledges, operational checklists etc. (The reader may wish to refer to the Privacy. SAFE assessment and compliance kit, copies of which are available from the PCO).

8.3
The E-Privacy Strategic Planning process
needs to operate in parallel with a Privacy Impact Assessment ("PIA"). In the absence of a common definition, a PIA may be described as a systematic process that evaluates proposed initiatives or strategic options in terms of their impact upon privacy. To be effective a PIA needs to be an integral part of the project planning process rather than an afterthought. The purpose of this assessment is twofold.

- To identify the potential effects that a project or proposal may have upon personal data privacy e.g. the introduction of a multi-purpose smart card.

- Secondly, to examine how any detrimental effects upon privacy might be mitigated.

8.4
PIA is a process that may be applied to a wide range of E-Business proposals that may be intrusive in terms of reasonable expectations of privacy, or the privacy rights enshrined in the Ordinance. It has equal validity applied to a public policy initiative e.g. electronic road pricing, as it has to a corporate initiative e.g. online customer profiling for prospecting purposes.

85
A PIA needs to commence at the outset of any planning initiative, strategy or policy proposal. Although the approach taken to PIA may vary with the context in which it is undertaken that approach should be methodical. Experience indicates that it should begin with definition of the problem or statement of issues. There are distinct advantages in outsourcing a PIA study not the least of which is that it lends impartiality to the process. This may be critical in influencing consumer or public opinion. For example, in the public sector the findings of a PIA study might be incorporated in a public consultation exercise, or policy position statement. This suggests that PIA is not an end in itself.

8.6
The outcome of any PIA should be measured against the influence it exerts upon proposals and strategic decision making. Ultimately the purpose is
to ensure that decision-makers are cognizant of the privacy dimension and work towards decisions that are privacy enhancing.

8.7
PIA has been referred to by a leading figure in the privacy community as an "early warning system". Approached correctly a PIA should ensure that organisations avoid the pitfalls that are implicit in a less disciplined approach to privacy issues. More significantly, as E-Business volumes grow, PIAs will contribute to protecting the image, goodwill and public confidence in those organisations that offer their services online.

Stage 3 Implementation of E –Privacy Strategies

9.1
Stage 3 moves the process forward to the
acid test of all planning exercises i.e. Does the organisation have the capability to execute the plan and accomplish the goals set? The proof of that ability is in the details and the managerial expertise demonstrated during the progressive roll-out of a strategy. Although the planning process has been outlined at the generic level, it is not the intention of this handbook to explore the functional strategies that might fulfil particular objectives in the E-Business marketplace e.g. the Marketing Mix strategy. That aside, recent experience of dot.coms suggests that there is no obvious strategic success formula in an environment characterised by considerable volatility. Many of the lessons are based upon hard experiential learning, rather than the discovery of an infallible blueprint.

9.2
As website content and services are usually directed at specific market segments, the opportunity should be taken to link E-Privacy to the formulation and implementation of consumer-oriented strategies. As one Marketing guru has noted, "The primary business of every business is to stay in business and to do that you have to get and keep customers".

It should be noted that, irrespective of the merits of any website strategy, the process of "getting and keeping customers" would only benefit from strategic formulations that address the following E-Privacy issues.

- The statutory provisions that confer personal data privacy rights on individuals, and set out best practice principles. Those principles should form the basis of a model E-Privacy contract between the provider and consumer.

- E-Privacy practices that are the product of consultation and consent rather than managerial edict.

- Technical specifications and systems architecture that have E-Privacy principles embedded in them.

- The development of an E-Privacy Policy framework that guides the design and implementation of provider strategies that target online consumers.

- E-privacy enforcement measures that ensure operational compliance on a day-to-day basis.

9.3
One response to the E-Privacy challenges confronting the provider in the formulation of functional or process strategies has been to develop systems that embrace Privacy-Enhancing Technology (PET). PET has, as its primary focus, the protection of

consumer identity or personal data. This is achieved through the deployment of a range of measures e.g. digital signatures, the creation of psuedo-identities and trusted third parties, that allow consumers to engage in Internet-based transactions without revealing their identity. These technologies are currently available in the marketplace and are not necessarily expensive to install. PET countermeasures have become increasingly sophisticated as software tools and have generally kept up with new forms of attack upon system integrity.

9.4
The appeal of PET is that it affords a high level of protection to personal data. In turn this may enable the provider to offer assurances to online consumers. It is precisely this type of proactive initiative, working in conjunction with an E-Privacy Policy, and good compliance measures, that adds value
to a website.

9.5
Finally, to manage vulnerabilities and challenges to the system, providers should develop effective auditing procedures. These need to address both technical and human components of the system and are designed to ensure that standard procedures are rigorously upheld and maintained. In short, that the system is secure and that it delivers the desired level of E-Privacy. For these conditions to be met personnel operating the system will need to adhere to strict guidelines.

Stage 4: The Pursuit of Excellence in E –privacy

10.1
The final stage in the E-Privacy Policy framework addresses three issues: the management of E-Privacy risks, the enhancement of compliance procedures, and the provider's commitment to continuous improvement. E-Privacy Policy is not only about engaging a systematic approach to online personal data privacy but is also concerned with the evolution of that approach to protect against new vulnerabilities. A long-term commitment to continuous improvement of systems security and the competencies of operational personnel is essential if new challenges are to be effectively countered.

10.2
Many providers have developed measures that have the power to raise the bar in respect of E-Privacy standards. Among these measures three in particular are worthy of note.

- **Risk Assessment and Review Procedures**

These procedures are designed to map security threats to the system. The better these threats are understood the more informed providers will be in terms of the controls that need to be applied to counter those risks. Risk assessment and review should become the raw input for better decision-making in respect of the integrity of the system, and the confidentiality of customer information stored
in databases.

- **Vulnerability Assessment and Review Procedures**

These procedures may be engaged during prototype systems testing, when piloting the website, or when the systems architecture is upgraded. Essentially the procedures use software to review systems capabilities with a view to discovering vulnerabilities or potential weaknesses so that preventative measures can be taken.

- **Incident Reporting Procedures**

The nature of system breaches e.g. hacking into databases, is such that it is not possible with complete confidence to predict where and when an attack will come from. It is therefore necessary to develop a means of policing network traffic to report on intrusions, or the suspicion of intrusion, and establish rapid-response protocols to deal with these situations. Damage control procedures have a direct value, in that they seek to minimise adverse effects, and an indirect value, in that they provide valuable lessons that can be built into training and future systems design.

10.3
The rate of change in IT means that new developments in software pose a continuous, if not growing, threat to system integrity and, by extension, to E-Privacy. Inevitably there will always be a small minority in the IT community that feel the need to demonstrate their 'skill' by penetrating 'secure' systems. And some will succeed. If providers wish to reassure their customers that their policy towards E-Privacy is uncompromised by such activities then it is incumbent upon them to install, maintain and enhance compliance procedures that will enable them to deliver on that assurance. This has been understood

by marketers of goods and services in the physical marketplace where manufacturers and retailers have endorsed their brands with extraordinary guarantees. These amount to a supreme level of confidence in the ability of the brand to satisfy consumer needs. In the cyber marketplace, for brand, read website. The challenge is for providers to be able to offer extraordinary guarantees that personal data privacy will not be infringed. To do that with any plausibility means that providers will need to uphold the letter of those guarantees and offer restitution if, and when, the conditions are violated. That is something that some may be reluctant to do because of the responsibility it places on the provider. However, that sort of thinking by providers will typify excellence in E-Privacy.

10.4

All systems thinking is premised on the understanding that a change in one part of the system will influence related part(s) of the system. It is conceivable therefore that in spite of the sophistication of IT systems and protocols E-privacy may be breached intentionally, or unintentionally, by the staff operating those systems. It is important therefore to sustain systems integrity by supplementing the processes outlined with a commitment to human resource training and development. The important point here is to recognise that no matter how well a training programme is designed and executed the real test of its effectiveness lies in the transfer of that training to the workplace. This means that good supervision,
and perhaps appropriate rewards, need to be part of the formula.

E–Privacy: The Pay-off

11.1
The systematic approach to E-Privacy outlined in this handbook necessitates the allocation of resources and that appropriation must be justified. It is reasonable therefore to offer a review of some of the benefits of imposing such a regimen on a provider's operations. It is against these benefits that the organisation can measure the efficacy of its IT, operational and human resource strategies, and their contribution towards the development of a professional approach to best practices in personal data privacy.

- **Building Trust and Confidence in the E-Economy**

Guaranteeing the exactitude with which personal data will be managed offers a means of building and sustaining high levels of trust and confidence in E-Business. If E-Privacy and the protection of personal data are demonstrated to be exemplary this will reflect favourably upon E-Brand equity and reputation. It may also facilitate growth by reinforcing loyalty and expanding the customer base.

- **Competitive Advantage**

The logical extension to this benefit is that providers will be able to use a high level of sustained trust and confidence as the basis for differentiating themselves from their rivals. Differentiation not only adds to the value of E-Brands and their positioning but also offers providers with a source of competitive advantage.

- **Proactive Approach to E-Risk Management**

The risks mentioned in Section 5 of this handbook exist. In particular there is every indication that the litigation risk will escalate. An investment in E-Privacy may therefore be regarded as one strategy for managing that risk.

- **Averting Intervention and Regulation**

If the parties to E-Business do not submit to high standards of voluntarily imposed E-Privacy protocols, and personal data protection, governments, or their regulatory agencies, are likely to step in to reinforce existing legislation and tighten up on statutory controls.

- **The Human Factor**

Employers need to provide clear leadership on E-Privacy issues. This can be achieved by championing the cause of an E-Privacy culture, and activating effective policies. Failure to do this will result in employees operating in an obscure work environment in which judgement calls substitute for thoughtful principles, and best practice procedures.

Annex The Data protection Principles

Personal Data (Privacy) Ordinance (Chapter 486)

The Data Protection Principles

Principle 1 - Purpose and Manner of Collection of Personal Data

(1) Personal data shall not be collected unless -
- (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
- (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
- (c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are -
- (a) lawful; and
- (b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that -
- (a) he is explicitly or implicitly informed, on or before collecting the data, of -
  - (i) whether it is obligatory or voluntary for him to supply the data; and
  - (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
- (b) he is explicitly informed -
  - (i) on or before collecting the data, of -
    - (A) the purpose (in general or specific terms) for which the data are to be used; and
    - (B) the classes of persons to whom the data may be transferred; and
  - (ii) on or before first use of the data for the purpose for which they were collected, of -
    - (A) his rights to request access to and to request the correction of the data; and
    - (B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

Principle 2 - Accuracy and Duration of Retention of Personal Data

(1) All practicable steps shall be taken to ensure that -
- (a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;
- (b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used -
  - (i) the data are not used for that purpose unless and until those grounds cease to be

applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data are erased;

(c) where it is practicable in all the circumstances of the case to know that -

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and

(ii) that data were inaccurate at the time of such disclosure,

--- that the third party -

(A) is informed that the data are inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

Principle 3 - Use of Personal Data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than -

(a) the purpose for which the data were to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a).

Principle 4 - Security of Personal Data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to -

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data are stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

Principle 5 - Information to be Generally Available

All practicable steps shall be taken to ensure that a person can -

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;

(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

Principle 6 - Access to Personal Data

A data subject shall be entitled to -

(a) ascertain whether a data user holds personal data of which he is the data subject;

(b) request access to personal data -

(i) within a reasonable time;

(ii) at a fee, if any, that is not excessive;

(iii) in a reasonable manner; and

(iv) in a form that is intelligible;

(c) be given reasons if a request referred to in paragraph (b) is refused;

(d) object to a refusal referred to in paragraph (c);

(e) request the correction of personal data;
(f) be given reasons if a request referred to in paragraph (e) is refused; and
(g) object to a refusal referred to in paragraph (f).