INFORMATION SECURITY POLICY

DOING THE RIGHT THING

DCC

1. PURPOSE OF THIS POLICY

This Policy defines a set of key information security principles and requirements which DCC companies are expected to comply with in order to protect our IT systems and data. The key principles are:

- **Confidentiality** – Ensuring that sensitive data is protected on the basis of 'least privilege', meaning that such data is accessible only to those who require access to it as part of their job;
- **Integrity** – Safeguarding the completeness and accuracy of data and key system reports; and
- **Availability** – Ensuring that important or critical data and IT systems are available to users when required.

Information security breaches could have a severe financial, operational, or reputational impact on our business. As such, it is important that all of our employees (and especially those working in IT teams) help us to avoid such breaches by adequately protecting the confidentiality, integrity, and availability of our IT systems and data.

2. WHEN DOES THIS POLICY APPLY?

This Policy applies to all DCC Group companies. The director with responsibility for IT in each business is required to ensure compliance with it.

This Policy is intended for use by local IT Teams in each DCC company. It is not an end user focussed document and is not required to be shared with end users. End users should primarily be referred to their local Acceptable Use Policy (or equivalent) if they have questions on information security matters.

3. WHAT THIS POLICY COVERS

The scope of the Policy includes, but is not limited to, all locally managed IT systems. This will typically include the network, email system, ERP system, IT hardware, mobile devices, etc. Where a DCC company has outsourced an important part of their IT environment to a third party service provider, they should also ensure that the third party complies with this Policy.

The topics covered in this Policy are aligned with relevant IT best practice frameworks such as: ISO 27001 and COBIT. The DCC Group Target IT Standards elaborate on the requirements within this document, providing clear and practical actions to enable IT teams achieve Policy compliance.

This Policy, and the Target IT Standards, cover critical areas of information security such as backups of systems and data; IT disaster recovery; technical security controls; user access management; network security; physical security; environmental controls; IT change management; and compliance with IT related compliance obligations (e.g. data protection, PCI DSS, etc.).

4. ASSURANCE

The primary means of assessing Policy compliance is via the DCC Group Target IT Standards. The Target IT Standards has three levels (Gold, Silver, or Bronze) with different standards applying depending on the size and risk profile of the business. They were set to enhance the level of IT control across a broad spectrum of IT environments across the Group. Each business is expected to achieve the relevant target compliance level in the Gold, Silver or Bronze versions of the Standards that apply to their business.

Compliance with the Policy will be tested by Group Internal Audit on a periodic basis. Results of audit testing will be reported to local management and also to DCC Group (via the Executive Risk Committee and Audit Committee).

5. WHY COMPLIANCE IS IMPORTANT

By complying with this Policy, each DCC company will have taken reasonable steps to protect their IT systems and data from security threats, whether internal or external, deliberate or accidental. This should enable each DCC business to prevent, and manage to an acceptable level, the potential impact of information security breaches. This will protect our business, our employees, our customers, and suppliers. Compliance is also important to ensure that we meet relevant legal, regulatory, and contractual obligations.

6. INFORMATION SECURITY POLICY REQUIREMENTS

6.1 INFORMATION SECURITY POLICY

- DCC will maintain a set of information security policies and standards, including this Policy. The objective of this is to provide DCC companies with guidance so that they can put appropriate measures in place in order to protect the confidentiality, integrity, and availability of their IT systems.

- This Policy applies directly across the Group to all DCC companies and compliance with it is mandatory. The director with responsibility for IT in each DCC company is required to ensure that all members of their IT teams and / or relevant third party contractors and consultants have been briefed on it.

- Compliance with the Target IT Standards is also mandatory. Each DCC company is required to achieve the relevant target compliance level in the Gold, Silver or Bronze versions of the IT Standards that apply to their business.

- In addition to this Policy and the Target IT Standards, both of which are mandatory, DCC Group will maintain a variety of information security policy templates covering particular areas of IT security. These templates compliment this Policy and the Target IT Standards and may be directly adopted as local policies or else tailored to suit the needs of the business as required. Use of these policy templates (e.g. the Network Security Policy template) is optional, however, in certain cases you must use the template or an equivalent in order to meet a relevant IT standard. All of these documents are available from the DCC Group IT Security Advisor and are also stored on the DCC Group IT Security SharePoint site.

6. INFORMATION SECURITY POLICY REQUIREMENTS (CONTINUED)

6.2 ORGANISATION OF INFORMATION SECURITY

Information security responsibilities for each Group business must be clear and unambiguous. Unless otherwise agreed with the Group CIO, the following applies:

- The director with responsibility for IT in each DCC company is responsible for ensuring that their IT processes, procedures, and controls are in compliance with this Policy and the relevant Target IT Standards that apply. Any significant known areas of non-compliance should be reported to and discussed with DCC (either the CIO or Group Internal Audit).

- Each company is required to have a local 'IT Security Officer'. The director with responsibility for IT in each DCC business should assign this role to an individual in their business (either themselves, a member of their IT team, or another suitable member of staff).

- A DCC Group IT Security Advisor is available to assist DCC companies in the execution of IT security policy and design of their cyber security processes and controls. However, each DCC company remains accountable for information security in their organisation.

- DCC Group will provide guidance on the role and responsibilities of the local IT Security Officers.

6.3 HUMAN RESOURCE SECURITY

- End user responsibilities for information security should be made clear to all staff. Each DCC company is required to have an end user focussed acceptable use policy (which may be based on the DCC Group policy template or an equivalent) which is readily available to them.

- All users of IT systems, including staff but also temps and contractors, should be asked to sign the acceptable use policy (electronically or physically) before they are granted access to the IT systems.

- All users should receive appropriate IT security awareness education as relevant for their job. For larger DCC companies, this should be supplemented with more formal security training.

- Updates to the acceptable use policy should be communicated to users on a regular basis. It should be made clear that breaches of policy will be subject to disciplinary procedures.

6.4 ASSET MANAGEMENT

- Each DCC company is required to have accurate and up-to-date registers of their key IT assets including IT hardware assets (servers, computers, and portable IT devices) and software assets (software installations and software licenses). An automated IT asset inventory tool should be deployed to ensure that listings of hardware and software assets are kept up-to-date.

- Each DCC company must know what its most sensitive data assets are. This should be documented in a Data Classification Register or Listing of Sensitive Data. Each DCC company must ensure that appropriate levels of security controls are in place to protect information assets. In particular, the most sensitive data should be tightly secured (e.g. access to shared Finance or HR drives should be restricted to relevant staff only).

- When no longer required, IT assets should be securely disposed of in a timely manner. Any excessive build-up of legacy IT assets (e.g. old laptops, PCs, servers, and backup tapes) will be considered a breach of this Policy unless there is a compelling reason for it (e.g. an ongoing legal investigation).

6.5 PORTABLE IT DEVICE SECURITY

- Each DCC company should be clear on which portable IT devices it allows and agrees to manage on its IT network, e.g. laptops, smartphones, tablet computers, and removable storage devices.

- Appropriate security controls are required to be implemented to ensure the security of such portable devices.

- All portable devices are required to be configured in line with a good practice security configuration standard (also known as a "security baseline" or "security hardening"). In particular:

  Laptops: all laptops are required to be encrypted (full disk encryption);

  Smartphones / Tablets: a MDM (Mobile Device Management) or EMM (Enterprise Mobility Management) solution should be in place capable of implementing a security policy to protect corporate data on mobile devices; and

  USB keys: the ability to transfer data from company networks / computers onto USB enabled devices should be restricted. Data stored on USB devices should be encrypted either by using an encrypted key or by using software which encrypts the data on the device.

6. INFORMATION SECURITY POLICY REQUIREMENTS (CONTINUED)

- Each DCC company is responsible for determining a suitable approach to 'bring your own device' security (or "BYOD"). However, if any DCC company decides to allow BYOD, it must ensure the security of any DCC data stored on those devices. The security on such devices should meet equivalent standards to corporate IT equipment (i.e. strong authentication, device encryption, etc.). Similarly, any use of BYOD must not introduce unacceptable risks (such as malware) onto the corporate networks.

6.6 ACCESS CONTROL

- Access to DCC systems and data is required to be appropriately managed. Access should only be authorised based on business need, security requirements, and the principle of least privilege. Access to sensitive data should be strictly on a need to know basis.

- Such access is required to be managed through strong identification and authentication controls (including unique user IDs and strong passwords). Appropriate technical controls, e.g. system enforced password policies, should be in place to ensure strong passwords are used and changed periodically. This should be backed up with relevant end user training and awareness to prevent 'complex' but easily guessed passwords (e.g. Password1).

- Formal user access management (UAM) processes, including business management authorisation of access setups, are required to be in place to prevent unauthorised access to systems.

- Access to sensitive systems, e.g. ERP or banking systems, should be role based where possible.

- Each local DCC IT team and HR team are jointly responsible for promptly updating or revoking access rights if users change jobs or leave.

- Access to DCC systems and data should also be periodically reviewed at regular intervals and annually at a minimum.

- Each DCC company must appropriately restrict access to powerful system accounts (Domain Administrators, DBAs, ERP system administrators, etc.) and review access to such accounts on a regular basis.

DOING THE RIGHT THING

6.7 CRYPTOGRAPHY

- When securing sensitive data (either at rest or in transit) there should be proper and effective use of cryptography to protect the confidentiality, authenticity, and integrity of the data. This should include using enterprise standard encryption software and (where relevant) good practice key management.

6.8 PHYSICAL AND ENVIRONMENTAL SECURITY

- Appropriate physical security measures must be put in place to prevent unauthorised physical access, damage, and interference to DCC information and information processing facilities. This may include security perimeters, access control systems, visitor access policies, etc.

- Appropriate environmental controls must also be put in place to reduce risks arising from environmental threats and hazards such as fire, floods, extreme temperatures, excess humidity, etc.

6. INFORMATION SECURITY POLICY REQUIREMENTS (CONTINUED)

6.9 OPERATIONS SECURITY

- Each DCC company is responsible for ensuring appropriate protection is in place to protect IT systems from malicious software. This will include, at minimum, the use of enterprise standard anti-malware systems across the IT estate.

- All DCC companies should maintain adequate and verified backups of their systems and data. Suitable backup processes and schedules are required to be in place.

- Copies of essential business systems and data are required to be taken regularly and stored at a separate location from the primary data or system location. At a minimum, all critical data should be backed up at least once daily.

- Daily backup checks should occur and backup failures are required to be investigated and resolved in a timely manner. Backup processes are also required to be regularly tested to ensure that they can be relied upon for emergency use when necessary.

- Each DCC company should ensure that appropriate audit logging and monitoring is configured. This will normally include event logs recording user activities, exceptions, system faults, system administrator activities, etc. Automated alerting should also be implemented, particularly on critical IT systems or systems dealing with highly sensitive data.

- The clocks of all relevant IT systems should be synched with an agreed time source. This is necessary to ensure the accuracy of system logs which may be required for incident investigations.

- Only authorised and licensed software should be installed on DCC networks. When possible IT teams should implement restrictions to prohibit the installation of unlicensed and unauthorised software by staff (i.e. restricting local administrator rights on PCs).

- All DCC companies, particularly larger and more IT dependent ones, should proactively monitor IT capacity requirements to avoid unplanned downtime or poor system performance.

6.10 NETWORK AND COMMUNICATIONS SECURITY

- DCC networks are required to be adequately managed and controlled in order to protect them from threats and to maintain the security of the systems and data residing on DCC networks.
- Firewalls and other security appliances are required to be used to protect DCC company networks and critical systems from external attack.
- All external email and internet traffic is required to be scanned for malicious software and spam at the gateway.
- All internet facing systems (i.e. servers hosting company websites, VPN servers for remote access, etc.) are required to be segmented from the general network into a DMZ using a firewall or other appropriate security appliances.
- For remote access to assets on DCC corporate networks (e.g. a user logging on to access their file server from home) multi-factor authentication should be used to provide strong authentication controls. This may include the use of one-time PIN codes, access tokens, client certificates, etc.
- For access to email services from outside the corporate environment (e.g. webmail, OWA, Office 365, etc.) multi-factor authentication should be used.
- Transfers of highly sensitive data must only be performed over appropriately secure channels, e.g. secure ftp, point to point VPNs, transport layer security (TLS), email encryption, etc.
- Network traffic from external wireless networks or "guest" wireless access points must never traverse internal DCC company networks. End users should not be able to bridge from the guest wireless to the corporate local area network (LAN).
- Corporate wireless networks, if required to be used, must be appropriately secured and subject to periodic security testing (e.g. via internal penetration tests).
- Network configuration, including network diagrams and configurations should be formally documented and a process implemented to ensure they are kept current.

6. INFORMATION SECURITY POLICY REQUIREMENTS (CONTINUED)

- Each DCC company is required to complete regular internal and external vulnerability scanning. If vulnerabilities are identified, appropriate and timely remedial action should then be taken to reduce the risk to an acceptable level (e.g. by applying a security patch to the affected system).

- In addition to vulnerability scans, IT penetration tests are required to be carried out regularly by suitably qualified and independent security experts. The scope of these tests should include both internal and external security. Web application tests, firewall reviews, and social engineering tests should also be included within the scope of such testing on a rotating basis over a suitable period. Weaknesses identified must be remediated on a timely basis.

- Email monitoring should be implemented to monitor user activity for compliance purposes as well as for the potential leakage of sensitive data.

- Content filtering must be implemented at the internet gateway to block inappropriate content as well as to protect the internal network and systems from malicious websites.

6.11 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

- Information security requirements should be assessed and addressed early on in IT projects, particularly large and complex IT projects (e.g. new system implementations, company acquisitions, etc.).

- Changes to IT systems must be professionally planned, managed and controlled.

- For every significant change, a change request should be logged and tracked on a change log which provides an audit trail of the change from initial request to its ultimate deployment.

- Changes must not be made 'on the fly' or without appropriate levels of pre-planning and authorisation. Roll back planning should be performed before all changes, particularly significant or risky ones.

- The extent and nature of management control should reflect the degree of risk inherent in the change. However, at a minimum, all changes should be approved by a relevant manager (normally in advance of deployment). Larger or riskier types of changes should undergo at least some level of IT and user testing and sign-off before deployment.

- Separate development, test, and production environments should be maintained for critical applications. Where possible, the development of changes should be kept separate from the deployment of changes, with appropriate segregation of duties between the two.

- Operating systems and software should be patched with up-to-date and relevant security updates. All critical IT systems must be patched on a timely basis.

6. INFORMATION SECURITY POLICY REQUIREMENTS (CONTINUED)

6.12 SUPPLIER RELATIONSHIPS

- The outsourcing of any part of a DCC company's IT environment to a third party service provider (e.g. the use of cloud based IT systems or the use of a third party data centre) does not remove the obligation of each DCC company to ensure good information security practice.
- Each DCC company must be aware of who their key IT service providers are. They must also have an understanding of outsourced providers of business services with whom their organisation shares data with. This should be documented in a Third Party Register.
- Relevant IT service providers (e.g. those providing outsourced IT services, hosting arrangements, system support, consultancy services, etc.) should be provided with copies of this Policy, and supplementary local policies if applicable, and be informed that they are required to comply with them. As an alternative, third parties may choose to provide DCC companies with relevant IT assurance reports (e.g. ISO 27001 certification, PCI DSS certification, or a SSAE16/ISAE 3402 report) which verify that they comply with good standards of information security.
- Compliance by third party service providers with good standards of information security must be reviewed at the outset of the relationship. Security compliance should also be reviewed periodically thereafter, particularly for more critical providers or those with access to sensitive data.
- Where relevant IT assurance reports are not available, DCC companies should verify the security of higher and medium risk third party service providers by performing testing (e.g. vulnerability scans, penetration tests, etc.) or scheduling site visits (e.g. for data centre providers).
- DCC companies must take other reasonable steps around third party information security such as by ensuring that third parties sign confidentiality agreements before gaining access to any confidential DCC systems or data. In addition, the 'right to audit' should be built into third party contracts with IT service providers where possible.

- Only IT approved systems should be used in DCC companies. Local IT teams should work in conjunction with business management to ensure that security risks are not introduced through the use of unsecure cloud systems and services. When evaluating the potential use of cloud services, IT teams should consider relevant factors including the sensitivity of the data being processed, the criticality of the service, the reputation of the provider, the stability of the cloud system, etc.

6.13 INCIDENT MANAGEMENT

- Each DCC company should implement processes to identify and investigate information security incidents (e.g. implementing processes by which end users can report issues, putting in place logging and monitoring to be able to investigate issues when they occur, etc.).

- Each DCC company should consider the incidents reported to them and decide if they constitute a security breach that warrants further investigation and resolution. Significant incidents / breaches must be reported to DCC.

- A formal process should be in place to record all relevant information on major security incidents or breaches and collate information for necessary analysis and tracking.

- Information security incidents or breaches must be contained and corrective action taken to address the immediate risk identified. The level of response should vary in accordance with the severity of the incident or breach.

DCC Group will provide Incident Management Guidelines to Local IT Security Officers as required.

6. INFORMATION SECURITY POLICY REQUIREMENTS (CONTINUED)

6.14 BUSINESS CONTINUITY MANAGEMENT

- IT continuity arrangements must be in place in all DCC companies to ensure continued IT operations in the event of scenarios which may impact on normal operations (e.g. major fires, floods, cyber-attacks, hardware failures, etc.).

- A listing of critical IT systems and services must be maintained in a Business Impact Analysis (BIA) document or equivalent document. The BIA should consider the impact of an interruption of the IT systems on wider business.

- IT continuity arrangements must be documented in the form of an IT Continuity Plan or IT Disaster Recovery Plan (DRP) which details how the IT systems and data will be restored. These IT plans may form part of a wider Business Continuity Plan or Crisis Management Plan which is owned by the business.

- IT systems and services should be designed with appropriate resilience and redundancy to prevent IT outages in the first instance. However, IT disaster recovery facilities should also be in place. These facilities will usually include the capability to recover critical IT systems and services at an offsite location.

- There must be a clear understanding between the business and IT on the capabilities of the IT continuity arrangements in place. Recovery time objectives (RTOs) and / or maximum tolerable outages (MTOs) should be used to express the business requirements for IT systems recovery. Recovery point objectives (RPOs) should be documented, setting out the agreed data loss tolerances which have been agreed with the business. RPOs will be closely tied to the frequency of the systems and data backup process.

- If any significant limitations exist in the IT continuity arrangements, they must be formally reviewed and approved by senior business management up-to and including the local Managing Director.

- IT disaster recovery testing must be carried out regularly (with the frequency of the testing dependent on the size and risk profile of the business) or following any significant changes or upgrades to IT infrastructure. Results of testing should be documented and reviewed with business management to ensure the IT DRP meets the business requirements.

DOING THE RIGHT THING

6.15 COMPLIANCE

- DCC companies are required to take appropriate steps to ensure compliance with legal, statutory, regulatory, or contractual obligations relating to information security. In particular, DCC companies are required to comply with EU data protection rules, software licensing obligations, and appropriate PCI DSS requirements if customer credit cards are processed.
- The director with responsibility for IT in each DCC company is responsible for ensuring that their Managing Director and Board are briefed on their compliance with this Policy and the Target IT Standards. This should take place as part of the annual Target IT Standards self-assessment process before the self-assessment return is submitted to DCC.

7. QUESTIONS OR CONCERNS

If you are unsure about how to apply this Policy in practice, please contact any of the following people

Peter Quinn
Group CIO

Direct: +353 1 279 9485
Mobile: +353 86 831 4669
Email: pquinn@dcc.ie

Paul Rafferty
Group IT Internal Audit Manager

Direct: +353 1 279 9407
Mobile: +353 86 028 5294
Email: prafferty@dcc.ie

David Stewart
Group IT Security Advisor

Direct: + 44 1324 408 034
Mobile: +44 7919 547 229
Email: dstewart@dcc.ie

8. HOW TO RAISE A CONCERN

If you have a concern that this Policy is not being followed, you have an obligation to raise it. You can do this using any of the methods set out on pages 8 to 11 of our Business Conduct Guidelines.

Remember that you will always be supported for raising a concern about a potential breach of this Policy. Any form of retaliation or discrimination against a person who has raised a concern will not be tolerated.

NOTES

www.dcc.ie

DCC

DOING THE RIGHT THING