3 Remote gambling and software technical standards (RTS)

RTS 1 – Customer account information

To provide customers with easily accessible information about their current balances.

BetIndex have worked to a strict template of design. Within this template, the need for customers to easily access information on their current balances is a high priority. Players, when logged into a BetIndex site or playing any of the games provided on the site, have consistent access to their account and when in a game a display informing them of their current balance.
BetIndex accept deposits of GBP£ only. This information is only available once the player has logged in. Players are only provided with one account and this is used for all products.

Players, whilst logged in and playing a game are presented with a games screen which informs them of the current balance (all products), stake and total sum of their chosen wager.

RTS 2 – Displaying transactions

All gambling

To enable the customer to understand the value and content of their transactions.

a. Players are provided with the amount being gambled in the currency of deposit. BetIndex accept GBP£ only.
b. BetIndex do not convert the currency of deposit of the player.
c.

- **i.** Information about the value of the gamble is displayed appropriately.
  All transactions for play are displayed in the player's depositing currency i.e. GBP£.
- **ii.** BetIndex do not host poker tournaments
- **iii.** BetIndex do not provide lotteries

d. BetIndex do not provide subscription lotteries

RTS requirement 2B
a. The Player is presented with consistent information within all game products these include:

- **Game name** Displayed on the game page
- **Restrictions of play**
- **Instructions on how to play, including a pay table for all prizes and special features.** Accessible via a link on the game page. (BetIndex games do not have special features, paytables)
- **Current account balance displayed in currency.** Displayed on the game page
- **Unit and total bet.** Displayed on the game page

The bet denomination (and where applicable the tokenisation) of the game is clearly visible or can be easily deduced. The artwork either states the maximum bet. The minimum bet is either readily available or easily deduced.
b. BetIndex do not accept telephone bets
c. All of the above information is displayed as the default option
d. BetIndex do not provide subscription lotteries

RTS 3 – Rules, game descriptions and the likelihood of winning
Gaming (including bingo), lotteries and betting on virtual events

RTS requirement 3A

a. All games rules are available in the game pages via an accessible link
b. Explanations are available from accessible links within game pages and on the homepages of the site(s)
c. Restricted play devices at a minimum provide explanatory content via links or menus
d. Explanatory content includes:
i. Game name
ii. Game rules/explanation
iii. Restrictions on play, if any
iv. The number of decks in play for card games (BetIndex do not provide casino style games)
v. BetIndex do not provide progressive style prizes.
vi. Clear instructions are provided on how to interact with the game
vii. BetIndex do not provide players with metamorphic games
viii. BetIndex do not provide lottery games

RTS requirement 3B

a. The player is informed of the current state of play within the game client. The player is displayed information of the state of the current game i.e. Playing. The player is also kept aware of their progress within the game by a display.
The state of play in all games is clearly discernible
b. BetIndex do not provide bonus games.
c. BetIndex does not supply lotteries.

RTS requirement 3C

i. BetIndex provide a full description of how games work, the determination of winners and prize allocation contained within game rules, terms and conditions and pay tables**.**
ii. BetIndex games are decided upon movements on the financial markets. A winning bet is determined by the decisions made by the players. No RNGs are used to decide winning games or selections.
iii. The odds are displayed to the player.
iv. the probability (likelihood) of winning events occurring is contained within the games rules and pay tables.
In addition to Game Rules, Help pages may be provided and ‘Rollover’ pop ups to display functional descriptions or possible outcomes.

RTS requirement 3D

a. The amounts players can win are displayed prior to making a bet.

b. BetIndex do not provide peer-to-peer games.
c. BetIndex game clients operate fix prizes.
d. Pay tables, game rules and help pages may display artwork or other supporting material.
e. Information is made easily accessible via hot links or pay tables, game rules and help pages.
f. BetIndex do not provide progressive prize games.

RTS 4 – Time-critical events
Gaming (including bingo), and betting on virtual events

RTS requirement 4A

BetIndex do not provide games where the speed of interaction has a significant effect on the customer's opportunity of winning.

RTS 5 – Result determination

RTS requirement 5A

a. The BetIndex system and games have been fully tested. Under normal operation, and in the absence of technical faults, the system and games will act in accordance with the rules.
b. All testing of new systems and product are conducted within a disciplined production and development environment. This is divided into development environment, staging environment and then moved to the 'live' environment after testing has been conducted. All games products are tested to comply with the published rules.
c. Customers are notified when errors that affect them, for example, incorrectly settled bets, have occurred as soon as is practicable after the event occurs. The BetIndex back office enables BetIndex trained and vetted staff to correct incorrectly settled bets.

RTS 6 – Result determination for play-for-fun games
Gaming (including bingo), lotteries, and betting on virtual events

RTS requirement 6A

BetIndex do provide play-for-fun games, the logic employed in those games mirrors that of Play-for-real games.

RTS 7 – Generation of random outcomes
Gaming (including bingo), lotteries, and betting on virtual events

RTS requirement 7A

BetIndex games do not utilise RNGs

.

Mapping and scaling BetIndex games do not utilise RNGs

RTS requirement 7B

BetIndex games are implemented as described in the available rules. As far as is reasonably possible, games and events are implemented fairly and in accordance with the rules and prevailing payouts, where applicable, as they are described to the customer.

RTS requirement 7C

If a virtual event simulates a physical device, the theoretical game probabilities match the probabilities of the real device.

The display of the result of a game is not misleading or deceptive to the customer.
All game rules and artwork are accurate and all customers have the opportunity of achieving an advertised outcome.

RTS requirement 7D

BetIndex will not alter the rules, payouts and outcome probabilities of a virtual event or game while it is available for gambling, except as provided for in the rules of the game.
Any such changes will be brought to the customers attention via a pop up message displayed to the player when they log onto the system or the game which has been altered.
Any changes will be made in the development area of the system platform, tested within the test environment and then, when testing and certification is completed, will be moved to 'live'.
Unspecified rules and game changes will not be made.

RTS requirement 7E

i) The display of the result of a game is not misleading or deceptive to the customer (i.e. does not improperly indicate a near miss).

ii) The outcome of each game is displayed for a reasonable length of time.

iii) BetIndex confirms that in relation to prizes in artwork, the following applies:-

- The customer is made aware of the amount wagered, the amount won and the event determination i.e. whether they have won or lost.

iv) Game wins are shown in British Pounds only.

RTS 8 – Auto-play functionality
Gaming

RTS requirement 8A

BetIndex does not utilise an auto play function.

RTS 9 – Skill and chance games with auto-play
Gaming

RTS requirement 9A

BetIndex games do not utilise an auto play function.

RTS 10 – Interrupted gambling
Peer-to-peer betting and gaming (including bingo)

BetIndex do not provide peer-to-peer betting and gaming.

RTS requirement 10B

When normal operation is interrupted due to a fault or error, BetIndex takes measures to ensure that users are treated fairly and that they are aware of how they will be treated if interruptions occur. Specifically, BetIndex has an automated system for flagging when unexpected system flaws, faults, or errors occur, including a robust automated system for recovering from failures that cause interruptions to gaming. BetIndex voids games automatically or manually and suspends future games during fault periods. In the case of a fault, wagers are returned in full to the user

RTS 11 – Limiting collusion/cheating
Peer-to-peer gaming

RTS requirement 11A

BetIndex do not provide peer-to-peer games.

RTS 12 – Financial limits
All gambling

RTS requirement 12A

a. BetIndex do not provide telephone betting.
b. For other access media (including internet, interactive TV and mobile), customers can contact customer support and impose any limitation on their account which they desire.
c. Limits
i. Deposit limits: players can request a deposit limit. The deposit limit is immediately active. If a player chooses to relax a limit it becomes active 24 hours later.
ii. Spend limits: See, Deposit limits above point (i)
iii. loss limits: N/A
d. The period/duration of the limit will be no less than one day (or 24 hours).
e. In addition:
i. As well as being able to set deposit limits players can request the disablement of their ability to play on the BetIndex product/site.
ii. Deposit Limits are imposed across all products.
iii. The ability to set a financial limit is available via the player account page.
iv. Players will always have access to the Contact Us link of Player Account link in the footer of the game page.

RTS requirement 12B

a. Any relaxation of a player limit i.e. a player wishes to increase their spend, is subject to a 24 hour cooling off period.
b. Any strengthening of a player limit i.e. a player wishes to reduce their spend, is effective immediately.

RTS 13 – Time requirements
All gambling except telephone gambling

RTS requirement 13A

The BetIndex system does not use a default full screen client application that obscures the clock on the customer's device.

a. Time of day will be taken from the customer's own device or 'server time' and is displayed in hours and minutes.
b. BetIndex will not detect whether or not customers have hidden their clocks.
c. Elapsed time will be displayed in minutes and hours.
d. For restricted display devices, time of day or elapsed time will be displayed where the device supports it.

RTS 14 – Responsible product design
All gambling

RTS requirement 14A

BetIndex products do not actively encourage customers to chase their losses, increase their stake or increase the amount they have decided to gamble, or continue to gamble after they have indicated that they wish to stop.
a.
i. the BetIndex system does not allow the amount of funds taken into a product to be topped up without the customer choosing to do so on each occasion.
ii. written or graphical information does not encourage customers to try to win back their losses
iii. customers who have chosen to exit a game are not encouraged to continue playing by, for example, being offered a free game.
b. N/A

4 Information provision annex (IPA) standards
IPA 1 – Customer account information

IPA requirement 1A

a. Each player account has an event report called the Account History accessible by accessing the My Account function – which highlights the movements in the customers' balances and incorporates real money credits, cash-ins (withdrawals) and wagering movements. The system also tracks each attempted deposit a player makes and if a deposit is rejected it will provide a reason which is as detailed as the processing merchant provide.

b. Players on the BetIndex system have access to tools which allow them to track their complete gambling activity via the “Account History” tab.
c. BetIndex customers do not move funds between products.
d. BetIndex does not provide telephone betting.
e. For gaming, where detailed historic game information is not necessarily directly available to customers, customers have easy access to details of the last game played and summarised information for previous activities.
f. For restricted display devices, customers that cannot access account history information will be supplied details by post if requested.

IPA 2 – Displaying transactions – third party user-interfaces

IPA requirement 2A

All third party products supplied to BetIndex must conform to BetIndex’s own product requirements, be independently tested and certified. Therefore, players will be supplied with all the information relevant to BetIndex games and will not have any information withheld, in particular with regard to transactions.

IPA 3 – In-running betting
Betting and peer-to-peer betting

IPA requirement 3A

BetIndex do not provide In running betting and peer-to-peer betting

IPA 4 – Use of automated gambling software
Peer-to-peer gambling

IPA requirement 4A

BetIndex do not provide peer-to-peer gambling

IPA requirement 4B

BetIndex do not provide Betting and peer-to-peer gambling

IPA 5 – Time-critical events
Gaming (including bingo), betting on virtual events, and peer-to-peer betting
IPA aim 5

IPA requirement 5A

BetIndex do not provide time critical events to customers.

IPA 6 – Interrupted gambling
Gaming (including bingo), betting on virtual events, and peer-to-peer betting
IPA aim 6

IPA requirement 6A

Customers are informed about BetIndex's policies with regard to interrupted gaming in BetIndex's Terms and Conditions on their site(s). Terms and Conditions are continuously available from all game event pages.

IPA 7 – Limiting collusion/cheating
Peer-to-peer gaming
IPA aim 7

IPA requirement 7A

Customers are informed about BetIndex's policies with regard to cheating in BetIndex's Terms and Conditions on their site(s). Terms and Conditions are continuously available from all game event pages.
BetIndex do not facilitate peer-to-peer gaming

5 Remote gambling and software technical standards – security requirements

Security requirements summary

A.5 Security Policy

Objective A.5.1 Information security policy

See Appendix 5.1. Security Policy Document

Requirement A.5.1.1 Information security policy document

The BetIndex Security Manager is responsible for the implementation and enforcement of the Security Policy. This includes the management of day-to-day activities related to the implementation and monitoring of compliance to the Security Policy. The main tasks include:

- Monitoring and reporting on the state of information security within BetIndex
- Ensuring that the Information Security Policy is implemented throughout BetIndex
- Developing and enforcing procedures to maintain security
- Ensuring compliance with relevant legislation
- Ensuring that BetIndex personnel are aware of their responsibilities and accountability for information security through the provision of training/awareness raising
- Monitoring for actual or potential information security breaches. Detailed responsibility for particular systems or business operations will be delegated to the relevant managers.

BetIndex has produced a Security Policy which will be distributed to all staff and relevant external parties.

Requirement A.5.1.2 Review of the information security policy

BetIndex's Security Policy will remain under a planned review process or will be revisited after significant changes occur to ensure its relevance. This process will take place at least once per year.

A.6 Organization of information policy

A.6.1 Internal organization

A clear understanding of the perceived threat is necessary, along with effective Information Assurance policies and procedures, assignment of roles and responsibilities, commitment of resources, training of critical personnel (e.g. users and system administrators), and personal accountability.

This includes the establishment of physical security and personnel security measures to control and monitor access to facilities and critical elements of BetIndex's Information Technology environment. However, most importantly, management will actively support security within the organisation. Initially this will be achieved by senior management's support and cooperation with the Security Manager or Compliance Manager in adhering to the Security Policy controls and guidelines.

Requirement A.6.1.8 Independent review of information security

This Security Policy manual, its implementation and systems will be subject to periodic review by both internal and external auditors, the recommendations from which will normally be implemented unless specific dispensation is given at the BetIndex management level. An external audit will be conducted at least once a year.

A.8 Human resources security

A.8.2 During employment

A.8.2.2 Information security awareness, education and training

Management responsibilities

Management must:

Ensure that all current and future staff are instructed in their responsibilities relating to the security of information.

- Ensure that all staff using production computer systems/media are trained in their use.
- Ensure that no unauthorised or untrained staff are allowed to access any of BetIndex systems, both computerised and paper based.
- Written authorisation should be submitted to the Security Manager, for any staff, including temporary staff, requiring access to BetIndex's Information systems prior to access being given.
- Determine which individuals are to be given authority to access specific computer systems. Where the system allows it, the level of access to specific systems should be on a job function need.
- Implement procedures to minimise BetIndex's exposure to fraud/theft/disruption of its systems, such as segregation of duties/dual control/staff rotation in critical susceptible areas.
- Ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability.

- Ensure that staff are aware of the need to declare any potential personal conflicts of interest. For instance, an individual working on an IT procurement assignment should make it known if they or any close relatives have direct interest in a potential supplier.
- Prior to an employee leaving, or to a change of duties, managers should ensure that:
    - Passwords are removed or changed as appropriate
    - Relevant partners or departments are informed of the termination or change, and the name is removed from authority and access lists
    - Reception staff and others responsible for controlling access to appropriate premises, are informed of the termination, and are instructed not to admit in future without a visitors pass
    - In rare cases it may be appropriate to assign staff to non-sensitive tasks whilst working out their notice
    - BETINDEX property, including information, is returned. Particular attention should be paid to the return of items that may allow future access. These include personal identification devices, cards, keys, passes, manuals and documents.

Staff responsibilities

- Each BetIndex employee is personally responsible for ensuring that no breaches of information security result from their actions
- Each BetIndex employee should declare any potential conflicts of interest
- Each BetIndex employee must take responsibility for accessing only areas of a system required to fulfil their job function and not access areas within the system, which hold data not relevant to their work
- Information is a major asset of BetIndex. All staff have a duty and responsibility to BetIndex, its customers and to fellow colleagues to protect this asset from unauthorised use, disclosure, access, modification and destruction
- Under no circumstances can staff sell or otherwise disclose BetIndex information for personal profit or gain
- Each employee must ensure that the person receiving information is authorised to receive it, where there are doubts checks should be made to ascertain the identity of the recipient prior to disclosure
- Employees must report any breaches of security or security incidents to their line manager and/or the Security Manager immediately
- Wherever possible, sensitive data must be cleared from desks and computer screens blanked when workstations are unmanned
- Staff who leave BetIndex must ensure that all equipment and information is returned to their manager prior to leaving
- Staff who access computer systems must keep their password secret and never disclose them to colleagues
- Any electronic files containing sensitive data must be password protected using the facilities built into the local software

A.8.3 Termination or change of employment

A.8.3.3 Removal of access rights

Access privileges are modified or removed, as appropriate, when an individual changes job or leaves. The Security Manager is responsible for modifying or removing access privileges before an individual’s final employment date.

A.9 Physical and environmental security

A.9.2 Equipment security

Requirement A.9.2.1 Equipment siting and protection

All equipment required to operate the games are to be hosted by Heroku Inc, their corporate headquarters are located at: 650 7th Street, San Francisco, CA 94103 an approved PCI hosting facility.

Heroku's physical infrastructure is hosted and managed within Amazon's secure data centers and utilize the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

PCI
Heroku use PCI compliant payment processor Braintree for encrypting and processing credit card payments. Heroku's infrastructure provider is PCI Level 1 compliant.

Sarbanes-Oxley
As a publicly traded company in the United States, salesforce.com is audited annually and remains in compliance with the Sarbanes-Oxley (SOX) Act of 2002.

Penetration Testing and Vulnerability Assessments
Third party security testing of the Heroku application is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team.

Physical Security
Heroku utilizes ISO 27001 and FISMA certified data centers managed by Amazon. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely.

.

Requirement A.9.2.6 Secure disposal or re-use of equipment

Disposal and re-use of equipment is managed by AWS. AWS will replace and provide equipment as required.

A.10 Communications and operations management

Objective A.10.1 Operational procedures and responsibilities

Requirement A.10.1.4 Separation of development, test and operational facilities

The licensee's development team use Javascript and NodeJS under Linux and Windows.

The development environment uses the multiplatform Eclipse as the main environment and recommended Integrated Development Environment, but it is not mandatory, the team can use any other IDE with the reservation that the GIT Version Control projects have to be opened by the IDE without any setting change.

The first step of the development process is always analysing the requirements. The resulting requirements/functional specification is used as a reference during the development. Usually requirements may slightly change during the development process, therefore the architecture has to be as flexible as possible. Based on the requirements specification the architect designs the system and creates a system specification which covers the technical aspects of the implementation. The unique tasks will be assigned by the team leader and the developers work on the parts of the modules. During the development the architect is responsible for the incoming change requests, and leads them throughout the whole system plan. At the end of the implementation phase the testers recevie the product and based on their reports the developers make the final touches.

Technical Standards and the Regulatory Requirements of the UK Gambling Commission are discussed and adhered to throughout the entire design process to achieve compliance with the UK Gambling Commission.

All production software gets tested on a stage platform. This 'stage is a full duplicate of a production environment. Components are tested for validity and interaction in this environment before they are released to a production environment.

No operational data is used in the test environment. All data there is generated by test users and only used in the test environment.

All stage websites are password protected to prevent any customers accidently accessing the stage environment instead of live.

Objective A.10.2 Third party service delivery management

Requirement A.10.2.1 Service delivery

By default, third party access is prohibited. If third party access should be required, then the least amount of access required for them to perform their duties, is granted. In such cases the person/s are monitored by in-house staff and the access revoked after the given duties have been performed.

Requirement A.10.2.2 Monitoring and review of third party services

The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

Requirement A.10.2.3 Managing changes to third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risk.

Objective A.10.4 Protection against malicious and mobile code

Requirement A.10.4.1 Controls against malicious code

Malicious codes can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access, capture passwords or other confidential information e.g. user account information. Malicious code attacks are usually difficult to detect as certain viruses can be designed to modify their own signatures after infecting a system and before spreading to another. Some can also modify audit logs in order to hide unauthorised activities.

The following are some examples of malicious code attacks:

1. Worms or viruses rapidly spreading through emails (e.g. I Love You, Melissa Virus);
2. Spying codes (e.g. Caligula Virus, Marker Virus, Groov Virus);
3. Remotely controlled codes (e.g. Back Orifice, NetBus); and
4. Coordinated attack codes (e.g. Trinoo, Tribe Flood Network (TFN)

The datacentre utilised by Heroku is ISO27000 and ISO19000 certified and malicious codes are prevented from breaching the Net benefit Firewall.

Requirement A.10.4.2 Controls against mobile code

Objective A.10.5 Back-up

Mobile codes are a deliberate attempt to destroy or damage data on a computer system. They are transmitted in software, which is innocently loaded onto a computer and can lead to complete loss of data on that system. BetIndex seeks to minimise the risks of computer viruses through education and good practice/procedures.

Recommended processes to prevent virus problems:

- Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.

- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

- Delete spam, chain, and other junk email without forwarding, in with the company's Acceptable Use Policy.

- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

- Always scan a floppy diskette from an unknown source for viruses before using it.

- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Requirement A.10.5.1 Information back-up

Databases are enabled with instant fallover by keeping a standby, in-memory replica, data is persistence is kept by keeping a snapshot, every 12 hours. Archive logs and transactions are also copied every 12 hours to a separate db instance for logs and transactions.

Objective A.10.6 Network security management

Requirement A.10.6.1 Network controls

Registering Users

In order that only the relevant personnel gain access to the systems they require, a formal application needs to be made to the IT Manager. Email requests/applications are acceptable. In the event email is used to register a user for a system, the authorising manager should send the email request/application directly to the IT Manager.

Access privileges are modified or removed, as appropriate, when an individual changes job or leaves. Access privileges are modified or removed before an individual’s final employment date. A leavers report is provided to the Security Manager from the Human Resources department, each month. The Security Manager notifies the relevant Systems Manager of any recent staff or contractor resignation or termination, where appropriate.

Password Policy

All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

- User accounts that have system-level privileges granted through group memberships should have a unique password from all other accounts held by that user.

- Passwords should not be inserted into email messages or other forms of electronic communication.

- All user-level and system-level passwords must conform to the guidelines described below.

General Password Construction <u>Guidelines</u>

Passwords are used for various purposes at the company. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e. dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - ○ Names of family, pets, friends, co-workers, fantasy characters, etc.
  - ○ Computer terms and names, commands, sites, companies, hardware, software.
  - ○ Birthdays and other personal information such as addresses and phone numbers.
  - ○ Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - ○ Any of the above spelled backwards.
  - ○ Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least seven alphanumeric characters long and is a passphrase (Ohmy1st).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Do not use the same password for the company accounts as for other non-the company access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various the company access needs. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share the company passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential the company information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to Network Administration and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by Network Administration or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Requirement A.10.6.2 Security of network services

Objective A.10.7 Media handling

Requirement A.10.7.1 Management of removable data

All PC users are advised to save their files to either available network drives or other removable storage media to ensure files are backed up each night. Users should also recognise that personal removable media are an increasingly inappropriate backup medium. Critical information that resides on users’ PCs should be configured to work with an over-the-network nightly backup process.

Requirement A.10.7.2 Disposal of media

All removable media such as CD-ROMs, memory sticks and removable drive disks, etc. should be reformatted before disposal, or properly destroyed.

Paper documents containing confidential information should be disposed of appropriately, when no longer required, either by shredding or by placing in a confidential waste bag provided by BetIndex.

Requirement A.10.7.3 Information handling procedures

Information handling procedures are managed by the Data Custodian. The Data Custodian will have responsibility for:

- Ensuring the system is operated in accordance with this policy
- The information held within their system is secure and used or disclosed in accordance with this policy and/or BetIndex’s Confidentiality Policy (relating to customer-identifiable information)
- Ensuring the accuracy and completeness of the data held within their system. In order to control data integrity, validation checks should be carried out periodically on all data held within the system
- That output data (e.g. printouts etc.) are used and disposed of in the appropriate way
- Ensuring that information is kept only for as long as is needed and archived appropriately.

Each set of data will be the responsibility of the Data Custodian and will include:

- Identifying all the data within the area of responsibility
- Agreeing who can access the data, and what types of access each user is allowed
- Determining the sensitivity level of the data
- Approving appropriate security controls
- Ensuring compliance with relevant guidelines with the Compliance Officer

Requirement A.10.7.4 Security of system documentation

This policy establishes requirements to successfully implement security protocols and procedures into the Systems Development Life Cycle (SDLC) to ensure that a system is developed in accordance with the stated requirements, works effectively, is cost effective, is secure, is compliant and is maintainable.

BetIndex will implement baseline security controls during the developmental life cycle of all IT systems, from the point of inception. The security controls selected for each baseline must achieve the appropriate level of protection. All SDLC plans and SDLC related documents shall be kept current.

Objective A.10.9 Electronic commerce services

Requirement A.10.9.1 Electronic commerce

Any e-commerce activities conducted on a BetIndex site is subject to the same conformity and controls as on-line transactions.

Requirement A.10.9.2 On-line transactions

BetIndex uses a 3rd party payment processor, provider Intelligent Payments based in Gibraltar.

Objective A.10.10 Monitoring

Requirement A.10.10.1 Audit logging

Where possible, systems should prohibit access after a maximum of 3 unsuccessful login attempts. All incidents where there have been two or three consecutive and unsuccessful attempts to login, should be recorded. This will provide an audit to enable the identification of malicious login attempts.

Audit Logs of information systems shall be reviewed regularly. Established reporting mechanisms shall be used to convey the results of the audit. Audit logs shall be archived on a regular basis and shall be retained until deemed unnecessary.

Security-related events must be logged and audit trails saved to Network Administration-approved logs. Security-related events include (but are not limited to) the following:

- User login failures.
- Failure to obtain privileged access.
- Access policy violations.

Requirement A.10.10.2 Monitoring systems use

- Every computer system will have an identified System Manager who will take responsibility for the security of the system and the data therein.
- System Managers must adhere to this policy and compliance guidelines.
- Access to BetIndexs information systems will only be given following authorisation from the Security Manager.
- All of BetIndex’s systems should have at least 2 individuals with the expertise to administer the particular system.
- System Managers will be responsible to the Security Manager for continued system security.
- Error reports should be produced regularly.

Requirement 10.10.3 Protection of log information

BetIndex’s information systems shall incorporate capabilities to log resource use with all logged activities identified by date and time of occurrence. Activity logs are kept securely and may only be accessed with the appropriate authorisation level

Requirement 10.10.4 Administrator and operator logs

The BetIndex’s Security Manager has authorisation to restrict access to system objects such as files, directories, devices, databases, and programs, based on user identity, least privilege, and a need-to-know. All access to BetIndex information systems shall be limited to only the resources that a user needs to complete or facilitate official duties. Access permissions shall be granted only by the Security Manager.

Requirement 10.10.5 Fault logging

We currently use git to manage issues or jira. The current workflow is when an fault is reported either by an end-user, developer or QA. A report of the fault is filed then assigned priority as well as severity. Progress of the fault including results, steps to reproduce as well as the code which fixes the fault is tracked in Giit or Jira. The priority of faults is dealt with by management and relevant technical staff or resources are assigned according to this to fix the fault. Once the fault is fixed, it will progress through the software development lifecycles with a record of the fix with each release.

Requirement A.10.10.6 Clock synchronization

Clock synchronisation is achieved via Universal Time (UTC) including scheduled leap second adjustments.

Standard – A.11 Business requirement for access control

Objective A.11.1 Business requirement for access control

NA.

All access to equipment is controlled by AWS.

Requirement A.11.1.1 Access control policy

Objective A.11.2 User access management

Requirement A.11.2.1 User registration

In order that only the relevant personnel gain access to the systems they require, the Security Manager oversees all user registration personally. The appropriate System Manager must be present and justify the registration requirement. In the event that email is used to register a user for a system, the authorising manager should send the email request/application directly to the Security Manager.

Access privileges are modified or removed, as appropriate, when an individual changes job or leaves. Access privileges are modified or removed before an individual’s final employment date. The Security Manager is responsible for modifying or removing access privileges before an individual’s final employment date.

Requirement A.11.2.2 Privilege management

Privilege management and access rights are managed by the Security Manager with the input from appropriate System Managers. As previously outlined above, BetIndex uses Heroku hosting services. This is an AWS managed solution. This eases the security workload for the Security manager.

1. Administrative Account Management
    a. Administrative accounts shall only be used for discrimination purposes to ensure that each administrative user is accountable for their actions by ensuring specific events can be associated with an authenticated UserID (i.e., non-repudiation). Login under generic system and administrative accounts is prohibited.
    b. Administrative accounts shall be limited and access controlled in accordance with BetIndex-established need-to-know concepts.
2. Administrative Password Guidelines
    a. Each BetIndex information system shall have a unique administrative password and the system must prompt for a change of the administrative password at least once every 90 days.
    b. Administrative passwords must not be passed in clear text across an internal BetIndex network or an external network.
    c. Prior to a system being put into production, default or temporary passwords used in testing shall be changed and documented.
    d. Administrative passwords will be curated by the Security Manager and kept in a physically secure location. Access to this list should require agreement from the Compliance Officer.

Requirement A.11.2.3 User password management

See Section A.11.3.1

Requirement A.11.2.4 Review of user access rights

The BetIndex Security Manager has authorisation to restrict access to system objects such as files, directories, devices, databases, and programs, based on user identity, least privilege, and a need-to-know. All access to BetIndex information systems shall be limited to only the resources that a user needs to complete or facilitate official duties. Need-to-know may be modified based on temporary assignments or projects with modifications requested or initiated by the Security Manager

Access control mechanisms shall, either by explicit user (manager) action or documented default, provide that objects are protected from unauthorised access. These controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing permission(s) to access sensitive information shall be granted only by the Security Manager.

System owners and system administrators are responsible for performing a review of access authorisation listings at least quarterly to determine whether they remain appropriate. This applies to operating systems and applications.

System owners are responsible for requesting updates on user employment from Human Resources (or equivalent) to ensure access and account privileges are valid. System administrators shall immediately remove or change access when users are terminated or transferred.

Objective A.11.3 User responsibilities

Requirement A.11.3.1 Password use

- Passwords shall not be distributed through non-encrypted electronic mail, voice-mail, or left on answering machines.
- Passwords for all systems, applications or processes shall be reviewed every 90 days.
- The use of automatic logon software to circumvent password entry shall not be allowed, except with specific approval from the Security Manager, for special tasks such as automated backups.
- Passwords shall be encrypted where appropriate for storage or transmission.
- Passwords used to access Internet or remote systems shall be different from passwords used to access internal systems and applications.
- Where appropriate, systems must require new users to change their temporary/default password after the first use of their account and/or after the password has been reset to a temporary/default password.
- Compromised passwords shall be disabled immediately upon detection and a new password issued.
- Before placing a system into a production environment, system administrators must change all default passwords and all passwords that were used in the development environment.

Requirement A.11.3.2 Unattended user equipment

IT equipment will not be taken off site, without formal approval from the Security Manager, other than to transport it from one of BetIndexs sites to another. Laptops/handhelds are vulnerable to theft, loss or unauthorised access and therefore users must ensure they demonstrate good security practices when taking them off site. In addition, all BetIndex laptops will be protected with a power-on password to prevent unauthorised access.

Objective A.11.4 Network access control

Requirement A.11.4.1 Policy on use of network services

This policy establishes the acceptable use of BetIndex's information systems. All network users shall make every effort to employ BetIndex information resources in an appropriate and acceptable manner.

Requirement A.11.4.2 User authentication for external connection

Remote users may not gain access to the internal BetIndex network due to the firewall policies in place.

Requirement A.11.4.3 Equipment identification in networks

Due to the size and location of equipment distribution within BetIndex, the need for equipment identification within networks is limited. Currently, a new device can only be added to the network manually using its Media Access Control address (MAC address). This is a unique identifier assigned to network interfaces for communications on the BetIndex physical network segment. However, as BetIndex expands its operational base and grows in size, automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

Requirement A.11.4.4 Remote diagnostic and configuration port protection

Physical and logical access to diagnostic and configuration ports shall be controlled. BetIndex does not allow remote access to its internal network

Requirement A.11.4.5 Segregation in networks

Due to the size and location of the BetIndex team, BetIndex has only one network and only one set of users and therefore does not segregate its network. Furthermore, as previously stated BetIndex does not provide remote access to its internal network via a remote connection. This provides an added layer of security. However, as the company grows, the appropriate changes will be implemented without delay.

Requirement A.11.4.6 Network connection control

BetIndex does not operate any form of shared network. Furthermore, the BetIndex network does not extend across the organisation boundaries. It is not possible for anyone to connect to the internal BetIndex network remotely due to the firewall and security restrictions in place.

Requirement A.11.4.7 Network routing control

BetIndex only operates a small internal network. As the networking requirements grow, routing control shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Objective A.11.5 Operating system access control

Requirement A.11.5.1 Secure log-on procedures

- BetIndex information systems must require each user to uniquely identify themselves and successfully authenticate to gain access.
- BetIndex information systems must not allow anonymous, guest, or shared account access unless authorised by the Security Manager.
- UserID configuration will be established based on the requirements of the information system.
- The naming convention for accounts must be standardised per system.
- Users shall not have different account IDs on the same system, i.e., one user account per user per system, unless authorised by the Security Manager; users with administrative privileges may have a second account specifically for the purpose of system administration.
- The system shall disable a user’s account following consecutive failed login attempts. Once disabled, the account must be blocked from access and scheduled to reset automatically or by administrator intervention.

- The system must invoke an automatic password-protected screen saver and provide users with the ability to invoke a password-protected screen saver on demand.

Requirement A.11.5.2 User identification and authentication

BetIndex data security and privacy shall focus on controlling unauthorised access to information. Data security shall be derived from three principles: confidentiality, integrity, and availability. These three principles emphasise the need for security to function properly in the BetIndex production environment.

In the context of this policy, the following provides the overall concepts and security principles for which all users are responsible. It is the responsibility of the Security Manager to define the specific mechanisms necessary to support these principles.

1. Accountability.
    a. All network, system, and application events shall be attributable to a specific and unique individual. A responsible individual must be assigned to every event using an identification service. An authentication service shall provide verification of this assignment and an audit service will trace any event, reconstructing the time, place, and circumstances surrounding it. In this context, identification refers to a security service that recognises a claim of identity by comparing a UserID offered with stored security information.
2. Authorisation
    a. All network, system, and application events shall only result from allowable actions through access control mechanisms. Permission may be derived directly from an individual's identity or from a job classification or administrative privilege based on that individual's identity. The principle of least privilege specifies that individuals only be granted permission for actions necessary to perform their jobs.
    b. Limiting actions to those properly authorised protects the confidentiality and integrity of data within the BetIndex production environment. In this context, access control refers to a security service that allows or denies a user request based on privilege, group information, or context.
3. Availability
    a. All permitted activity shall operate with reliability. Users must be able to retrieve the correct data necessary to perform such events. All event results shall be completed unless the event is totally aborted. Event results must not depend on unforeseen aspects of other simultaneous events. The security services themselves shall be documented and easily administered. In this context, reliability refers to a security service that guarantees data has not been altered, deleted, repeated, or rearranged during transmission, storage, processing, or recovery.

Requirement A.11.5.3 Password management system
See section 10.6.1

Requirement A.11.5.4 Use of system utilities

The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

Requirement A.11.5.5 Session time-out

User account sessions will time-out in the event of inactivity. This includes user connections to the Internet or to specific applications.

Requirement A.11.5.6 Limitation of connection time

User account sessions will lock-out during periods of inactivity and will require authentication to regain access.

Objective A.11.6 Application and information access control

Requirement A.11.6.1 Information access restriction

Passwords are provided to permit access to limited levels of information according to the needs of a member of staff. Access should be restricted to those staff directly involved with the input and retrieval of information.

The issues considered in establishing user access are as follows. Restricting access to:

- Specific data elements or records
- Named data about individuals
- Anonymised data about individuals
- Aggregated data
- User access to a particular "view" of the data
- Defining what a user can do with the data (i.e. create, read, delete, update)

All passwords are specific to individuals and are not disclosed to others. Temporary staff are given their own password, which is deleted when they leave.

Passwords within a BetIndex information system are changed regularly. Passwords must be changed periodically, and no password will exceed 6 month activity. The recommended period is 90 days activity. Passwords are changed whenever there is any indication of possible system or password compromise.

No individual is given access to a BetIndex system without first being made aware of their security responsibilities.
All access is subject to the BetIndex configured access list.

BETINDEX Configured Access Control List

XOX – Backend reporting/administration tool
CL - Support web interface
Game configuration (RAT)
Development systems
Hosting site

	XOX	CL-Support	RAT	Dev systems	Hosting sites

Game Management	x				
Marketing Management	x		x		
Accounts Management	x				
HelpDesk Management	x				
System Administrators					x
System Developers			x	x	x
Web Developers					
HelpDesk/24-hour support	x				
Chat Masters (CM’s)		x			
Chat Leaders (CL’s)		x			
CRM	x				

Requirement A.11.6.2 Sensitive system isolation

All BetIndex offices, employees, and contractors will identify and provide adequate security protection for all Sensitive But Unclassified (SBU)/Sensitive Security Information (SSI) information. As such, when necessary BetIndex will utilise encryption to defend sensitive systems and to prevent unauthorised disclosure of sensitive information to users.

For example, BetIndex uses 4096bit RSA encryption with Optimal Asymmetric Encryption Padding (OAEP). With this approach, there are two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext. Neither key will do both functions and there is no efficient solution to calculate one key from the other. The Security Manager shall exercise control over all keys utilised in encrypted transmissions. No SBU/SSI information should ever be transmitted in clear text.

The Secure Sockets Layer (SSL) specification is deployed to provide secured access to sensitive information on Web servers. When SSL is used to protect BetIndex sensitive information, the latest version shall be used with 128-bit encryption

Objective A.11.7 Mobile computing and teleworking

Requirement A.11.7.1 Mobile computing and communications

Issuing Policy

Personal Communication Devices (PCDs) will be issued only to the company personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

Handheld wireless devices may be issued, for operational efficiency, to the company personnel who need to conduct immediate, critical Company business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

Bluetooth

Hands-free enabling devices, such as the Bluetooth, may be issued to the company personnel who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters; Bluetooth 2.0 Class 1 devices have a range of 330 feet.

Personal Use

PCDs and voicemail are issued for the company business. Personal use should be limited to minimal and incidental use.

PCD Safety

Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If employees must use a PCD while driving, the company requires the use of hands-free enabling devices.

Requirement A.11.7.2 Teleworking

General Requirements

Teleworking is not considered an employee right and can be suspended at any time. The employee shall return all Trading Games Limited-issued equipment, software, and materials at the conclusion of the Telework arrangement.

BetIndex retains the right to inspect the home or alternate work-site and the equipment used by an employee to ensure that proposed work-sites are safe and that all equipment is adequately installed, maintained, and secured.

Data Access of Sensitive or Classified Data

It is not possible to access sensitive information stored on local BetIndex servers from a remote location. This is due to the firewall policies in place. Access to sensitive or classified data stored on remote servers is performed in exactly the same way in which it is accessed from BetIndex offices. It is subject to the same security restrictions and all data is encrypted through SSL during transmission.

Computer Security Requirements

Trading Games Limited-issued computers utilised in support of the Teleworking shall be loaded with the latest versions of appropriate and necessary software. Only an approved hardware/software configuration may be used by the teleworker and the teleworker is not allowed to modify the approved hardware/software configuration without prior approval from an appropriate manager.

In the event of a hardware failure, Telework participants shall comply with security procedures to protect BetIndex information stored on computer magnetic media when the computers are repaired or serviced. Where the hard disk of a computer is inoperable, arrangements shall be made to remove sensitive information from the hard disk prior to having the computer serviced.

Standard – A.12 Correct processing in applications

Requirement A.12.2.1 Input data validation

Data accuracy is the direct responsibility of the person inputting the data supported by their manager. Data relates to information held in computerised format and in manual records. Error correction and validation are performed at the point of input, as well as at the server where the data is stored. Data loss or corruption should be reported immediately to the Data Custodian.

Requirement A.12.2.2 Control of internal processing

BetIndex utilises multiple layers of security controls throughout its systems. These areas include, but are not limited to, network and infrastructure, boundaries (e.g. firewalls) and the computing environment via appropriate audit logging and access controls. Protection and detection measures are in place where necessary to ensure internal processing security.

There are three primary considerations when controlling internal processing:

1. Confidentiality: access to information is confined to those with specified authority to view the information
2. Integrity: information is accurate and kept up to date
3. Availability: information is available to the right person, when it is needed

BetIndex has obligations to maintain security and confidentiality of information, notably under The Data Protection Act. BetIndex has to ensure compliance with the Remote Technical Standards issued by the UK Gambling Commission.

Risk management

All BetIndex systems will be subject to periodic security reviews by systems managers or authorised member of staff (appointed by the Security Manager). The depth of a review will be determined by the importance and size of the particular system. The risk assessment should be documented, as should any problems that are identified. Action plans should then be developed for removing the weaknesses or introducing system or procedure change.

Reviews should include:

- Identification of assets of the system and their value to Trading Games Limited
- The sensitivity of the information being held on each information system
- The physical security of the facility within which information equipment is housed
- The physical hazards to which the system might be subjected (e.g. fire), including any additional hazards (proximity to danger areas)

- The ease with which non-authorised people could get access to information systems
- The potential for physical tampering (e.g. communication links)
- The strength of access protection mechanisms (e.g., password protection) and whether users are following security procedures
- The security of all communication links to the system (e.g. use of encryption)
- If the system audit trails are being logged (e.g. file usage logs)
- Whether users can electronically load data onto the system (e.g. copy files from removable media)
- The reliability of data entry protection functions (e.g. data integrity checks)
- The presence of unauthorised software
- The level of staff turnover and use of temporary staff
- Assessment of likelihood of threats occurring, including the temptation towards fraud, which the particular system could offer and the extent to which professional hackers might wish to gain access
- Assessment of the impact of an incident
- Assessment of the security risks that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets
- Identification of practical cost effective countermeasures/security systems.

Requirement A.12.2.3 Message integrity

BetIndex transmits information over a Secure Socket Layer (SSL) where appropriate. SSL provides server authentication, data encryption and message integrity. Without SSL, most web transactions, including credit card transactions, would travel across the internet as clear text, and could be copied, modified or deleted.

Requirement A.12.2.4 Output data validation

Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. This validation usually takes place as part of a testing process, prior to deployment. On-going testing is performed throughout the life-cycle of a system.

Objective A.12.3 Cryptographic controls

Requirement A.12.3.1 Policy on the use of cryptographic controls

Diffie-Hellman Key Exchange algorithm is used to create encryption keys for communication between game server and end-user client. Internal IGS communication such as the game server to the database server (which is located on the same machine/server inside the IGS) is done by fixed encryption keys.

Requirement A.12.3.2 Key management

i) Server to end-user client communication is done by Diffie-Hellman key generation. Keys are dynamically generated to run-time for each connecting client and as such not stored on disk.

ii) 3Des encryption is used, which is a 168 bit encryption algorithm. (3 x 56-bit keys, 168-bit key length, and 192-bit key storage).

iii) 3Des encryption algorithm is used. The equipment testing house did not raise the encryption algorithms used as an issue.

iv) Where a weakness in the DH or 3Des key system is found, then an investigation will follow for alternative implementations that fix the weaknesses or to find a new improved key handling system.