



Capability Statement.

We don't just do IT. We manage risk, ensure continuity, provide responsive support, offer clear guidance, and teach your team. Five pillars, and this document sets out everything we deliver under each one.

MANAGE RISK

ENSURE CONTINUITY

RESPONSIVE SUPPORT

CLEAR GUIDANCE

TEACH YOUR TEAM

PHONE

1300 900 222

EMAIL

support@bastionit.com.au

WEB

bastionit.com.au

CURRENT AS AT AUGUST 2026

IT that prevents the problem, not just bills for the fix.

Bastion IT keeps South East Queensland businesses connected and secure. We are owner operated, which means the person who scopes your work is the person accountable for it, and the service desk answering your call sits in Australia.

Most providers make money when things break. We think that is backwards. Our model is built on prevention, on knowing your setup well enough to spot the fault before your staff do, and on telling you the truth about where you stand. If your current IT is working, we will say so.

We supply the whole stack. Security, backup, networks, business internet, Microsoft 365, hosting, phone systems and the hardware itself. One provider, one bill, and one person accountable when something needs sorting.

That is not the whole list. If you need something that is not in this document, ask, because we would rather source it properly than have you buy it somewhere it cannot be supported.

WHAT WE COMMIT TO

✓ MONTHLY EXECUTIVE REPORTING

✓ LIVE 24/7 SECURITY OPERATIONS

✓ AUSTRALIAN-ONLY SERVICE DESK

✓ QUARTERLY ON-SITE REVIEWS

ACCREDITED AND CERTIFIED

SMB1001 GOLD

MICROSOFT PARTNER, BRONZE

3CX SILVER PARTNER

OUR OPERATING CADENCE

We don't wait for fires. Every pillar in this document is maintained with automated daily checks and 100% human verification weekly.

The Five Pillars.

Everything we do sits under one of five commitments. The services on the right are how each one gets delivered, and every one of them is a standing responsibility rather than a project with an end date.

01

Manage Risk

Most incidents are not clever. They are an account without MFA, a firewall nobody has patched, a camera system sitting on the same network as the file server. We close those gaps and we keep them closed.

BASTION CYBERSECURITY
MANAGED SECURITY TIERS
MICROSOFT 365 & IDENTITY
NETWORK & CONNECTIVITY
PHYSICAL SECURITY

02

Ensure Continuity

Continuity is not a backup job reporting success. It is knowing that your data, your systems, your phones and the machines your staff sit at will all still be working tomorrow, because somebody tested them.

BACKUP & RECOVERY
CLOUD SOLUTIONS
HOSTED INFRASTRUCTURE &
DOMAINS
BUSINESS TELEPHONY
HARDWARE & PROCUREMENT

03

Provide Responsive Support

When something breaks you want a person who already knows your setup, not a queue. One owner per ticket, an Australian service desk, and a named technical lead your team gets to know.

BASTION MANAGED SERVICES
SERVICE LEVELS

04

Offer Clear Guidance

You should understand what you are paying for and what is protecting your data. Monthly reporting you can actually read, quarterly reviews about what is coming, and honest advice even when it costs us the sale.

EXECUTIVE REPORTING
QUARTERLY REVIEWS
COST AND LICENCE CLARITY

05

Teach Your Team

A team that spots a dodgy email is your strongest security control. A team that knows how to use the tools you already pay for is your cheapest productivity win. We teach both, in sessions short enough that people actually turn up.

SECURITY AWARENESS
SOLUTIONS TRAINING

01

Pillar One

Manage Risk

Most incidents are not clever. They are an account without MFA, a firewall nobody has patched, a port left open because it was convenient. We close those gaps and we keep them closed.

SECURITY-FIRST MANAGED IT

Bastion Cybersecurity

THE PROBLEM

Standard MSPs often prioritise convenience over safety, leaving open ports and weak identities.

BUSINESS IMPACT

High risk of ransomware, data theft, and catastrophic insurance premium hikes.

THE BASTION FIX

Hardened identity controls, zero-trust network principles, and continuous vulnerability scanning.

- ☐ CONTINUOUS VULNERABILITY SCANS
- ☐ ENDPOINT PROTECTION (EDR)

- ☐ IDENTITY HARDENING
- ☐ PATCH VELOCITY TARGETS

SIGNS THIS APPLIES TO YOU

- ☐ Nobody can tell you which accounts still have no multi-factor
- ☐ Patching happens when somebody remembers
- ☐ You have never seen a vulnerability scan of your own network
- ☐ Your insurer has started asking harder questions

HOW YOU WILL KNOW IT IS WORKING

- ☐ Multi-factor coverage reported as a percentage every month
- ☐ Time from patch release to deployment, tracked
- ☐ Open vulnerabilities listed with an age against each
- ☐ Endpoint protection status for every machine

NEXT STEP: AUDIT CURRENT IDENTITY HYGIENE AND ENABLE 100% MFA ADOPTION.

IDENTITY & ACCESS

Microsoft 365 & Identity

THE PROBLEM

Microsoft 365 tenants are almost always left on default settings, with legacy authentication enabled, inconsistent multi-factor coverage, and no conditional access rules.

BUSINESS IMPACT

A single compromised mailbox gives an attacker your invoicing history, your supplier list, and a trusted address to send from. Payment redirection fraud follows.

THE BASTION FIX

Multi-factor across every account with no exceptions, conditional access policies that block sign-ins from where your staff never work, mailbox rule and forwarding monitoring, and licensing reviewed so you are paying for what you actually use.

- ☐ FULL MFA COVERAGE
- ☐ MAILBOX RULE MONITORING
- ☐ CONDITIONAL ACCESS POLICIES
- ☐ LICENCE OPTIMISATION

SIGNS THIS APPLIES TO YOU

- ☐ Staff sign in from anywhere with just a password
- ☐ Nobody has reviewed who holds administrator rights
- ☐ Legacy authentication has never been turned off
- ☐ You still pay for licences that left with former staff

HOW YOU WILL KNOW IT IS WORKING

- ☐ Every account confirmed on multi-factor, exceptions named
- ☐ Sign-ins from outside your normal locations blocked and reported
- ☐ New mailbox rules and forwarding flagged as they appear
- ☐ Licence count reconciled against headcount each month

NEXT STEP: A TENANT HEALTH CHECK COVERING MFA COVERAGE, LEGACY AUTHENTICATION, ADMIN ACCOUNTS, AND EXTERNAL SHARING SETTINGS.

CONNECTIVITY & PERIMETER

Network & Connectivity

We manage the network and we supply the internet service running over it, so there is never an argument about whose fault an outage is.

THE PROBLEM

Flat networks where the guest wifi, the security cameras, the payment terminals and the accounts machine all sit on the same segment, behind hardware nobody has updated since it was installed.

BUSINESS IMPACT

One compromised device reaches everything, and an internet outage stops the entire site because there was never a second path.

THE BASTION FIX

Segmented networks that keep cameras, guest access and operational equipment away from business systems, firewalls and access points that are patched and monitored rather than set and forgotten, and DNS filtering that blocks known-bad destinations before a click becomes an incident.

☐ NETWORK SEGMENTATION

☐ DNS AND WEB FILTERING

☐ MONITORED FIREWALLS

☐ MANAGED WIRELESS

WE SUPPLY THE INFRASTRUCTURE TOO

We supply the internet service and the equipment as well as managing them, across business grade connections, failover paths, switching, wireless and structured cabling. Scoped to the site in front of us rather than picked off a list.

SIGNS THIS APPLIES TO YOU

- ☐ Cameras, guests and the accounts machine share one flat network
- ☐ Nobody knows when the firewall was last updated
- ☐ A single internet fault stops the whole site
- ☐ The wifi drops in the same spot every week

HOW YOU WILL KNOW IT IS WORKING

- ☐ Segments documented, with what can reach what
- ☐ Firewall and access point firmware status reported
- ☐ Blocked destinations summarised each month
- ☐ Outage minutes and failover events recorded

NEXT STEP: MAP WHAT IS ACTUALLY CONNECTED TO YOUR NETWORK AND WHICH OF IT CAN REACH YOUR FILE SERVER.

SITE & PREMISES

Physical Security

Cameras, door access and alarms designed and managed as part of your IT, rather than bolted on by a separate contractor who never speaks to us.

THE PROBLEM

Cameras and door controllers get installed by whoever quoted cheapest, then plugged into the same flat network as the accounts machine, running default passwords and firmware nobody has touched since the day it went in.

BUSINESS IMPACT

Footage that turns out to be missing on the one day you need it, a camera system that becomes the way an attacker gets onto your network, and nobody who can tell you who currently holds access to which door.

THE BASTION FIX

Camera and access hardware kept on its own network segment away from business systems, firmware and credentials managed on the same schedule as the rest of your fleet, retention set to match what your insurer and your industry actually require, and one register of who has access to what.

- ☐ SEGMENTED CAMERA NETWORKS
- ☐ MANAGED FIRMWARE AND CREDENTIALS

- ☐ DOOR AND ACCESS CONTROL
- ☐ RETENTION SET TO POLICY

SIGNS THIS APPLIES TO YOU

- ☐ Your camera system runs on the same network as your files
- ☐ Nobody has changed the default password on a recorder
- ☐ You cannot say who currently holds access to which door
- ☐ Footage retention was set by whoever installed it

HOW YOU WILL KNOW IT IS WORKING

- ☐ Camera and door hardware confirmed on its own segment
- ☐ Firmware and credential changes logged with the rest of the fleet
- ☐ Access register reviewed and reissued as staff change
- ☐ Retention checked against what your insurer expects

NEXT STEP: CHECK WHETHER YOUR CAMERA SYSTEM SITS ON THE SAME NETWORK AS YOUR FILE SERVER, AND WHEN ITS FIRMWARE WAS LAST UPDATED.

Managed Security Tiers.

Our packaged security stack. Four tiers priced per device, each building on the one below, so you can start where your risk actually sits and step up later without replacing anything.

TIER	WHAT IT ADDS
Email Security	Advanced email threat protection and Microsoft 365 data protection, dark web monitoring for your domain and staff addresses, and ongoing online cyber security training.
Guardian	Remote monitoring and management, antivirus, endpoint detection and response, endpoint backup, and business password management.
Shield	Everything in Guardian, plus managed detection and response backed by a security operations centre.
Fortress	Everything in Shield, plus application control, mobile device and mobile application management, and full disaster recovery management.

WHAT SITS BEHIND THE TIERS

The tiers draw on a full set of controls covering identity, email, endpoints, mobile devices, monitoring and staff training. Which of them apply depends on the tier you sit on, and we will talk you through what your business actually needs rather than defaulting you to the top one.

Tiers are priced per workstation. Guardian and Shield are also available at a virtual desktop and server rate.

APPLICATION CONTROL, INCLUDED IN FORTRESS

Default deny, so only software you have approved is allowed to run. The single most effective control against ransomware, because it stops unknown code before it executes rather than trying to recognise it afterwards. It also governs what approved software is allowed to do once it is running, who can run something with administrator rights, what can be written to removable storage, and how endpoints are permitted to talk to the network.

02

Pillar Two

Ensure Continuity

Continuity is not a backup job reporting success. It is knowing, because it was tested last month, that you can be working again inside a time you agreed to in advance.

RESILIENCE & RECOVERY

Backup & Recovery

THE PROBLEM

Backups get configured once and then trusted for years. Nobody finds out they have been failing silently until the day they are needed.

BUSINESS IMPACT

Days of lost work, a ransomware negotiation you did not need to have, and an insurance claim that gets questioned because the controls were never tested.

THE BASTION FIX

Backup coverage scoped deliberately to the business data that matters, including cloud workloads and the work folders on endpoints, with restore testing on a defined schedule and a documented recovery process rather than an assumed one.

- ☐ CLOUD AND ENDPOINT COVERAGE
- ☐ DOCUMENTED RECOVERY PROCESS

- ☐ SCHEDULED RESTORE TESTING
- ☐ RETENTION REVIEWED ANNUALLY

WHAT WE COVER

Desktops, servers and Microsoft 365, scoped to what the business actually needs to be able to recover rather than everything by default.

SIGNS THIS APPLIES TO YOU

- ☐ You know the backups run, but not that they restore
- ☐ Nobody has tested a restore this year
- ☐ Microsoft 365 is assumed to back itself up
- ☐ There is no agreed figure for how long you can be down

HOW YOU WILL KNOW IT IS WORKING

- ☐ Date of the last successful test restore, every month
- ☐ Coverage listed against what the business actually needs
- ☐ Failures raised the day they happen, not at renewal
- ☐ Retention reviewed annually against your obligations

NEXT STEP: VERIFY THE DATE OF YOUR LAST SUCCESSFUL TEST RESTORE, NOT YOUR LAST SUCCESSFUL BACKUP.

SUPPLY & LIFECYCLE

Hardware & Procurement

We source, configure and deploy the hardware your team works on, then track it through its life until it is retired and wiped properly.

THE PROBLEM

Hardware gets bought ad hoc. A laptop from a retail store here, a machine from whichever supplier answered the phone there. Nothing matches, nothing is documented, and the warranty details live in somebody's inbox.

BUSINESS IMPACT

New starters wait days for a machine, faults take longer to diagnose because no two devices are set up the same way, and equipment quietly stays in service years past the point where replacing it would have been the cheaper option.

THE BASTION FIX

Standard device builds so every machine leaves us configured, encrypted and enrolled the same way, hardware sourced through our distribution accounts with the pricing shown to you honestly, and an asset register that tracks warranty and replacement dates before they turn into a problem.

- ☐ STANDARD DEVICE BUILDS
- ☐ ASSET AND WARRANTY REGISTER

- ☐ IDENTITY AND DEVICE ENROLMENT
- ☐ CONSUMABLES AND ACCESSORIES

SIGNS THIS APPLIES TO YOU

- ☐ No two machines are set up the same way
- ☐ Warranty details live in somebody's inbox
- ☐ New starters wait days for a working laptop
- ☐ You do not know how many devices are out of warranty

HOW YOU WILL KNOW IT IS WORKING

- ☐ Asset register carrying warranty and replacement dates
- ☐ One build standard applied to every new machine
- ☐ Devices near end of life flagged before they fail
- ☐ Spend visible per device rather than buried in a bill

NEXT STEP: ASK HOW MANY MACHINES IN YOUR BUSINESS ARE OUT OF WARRANTY RIGHT NOW, AND SEE IF ANYONE CAN ANSWER.

LICENSING & PLATFORM

Cloud Solutions

We supply Microsoft licensing ourselves, so your licences, your tenant and the people supporting it all sit with one company. No reseller in the middle who cannot actually fix anything.

THE PROBLEM

Licences get bought by whoever needed one at the time, often at retail, often the wrong plan, and nobody reviews them when staff leave. Support for the platform sits with a vendor who has never seen your setup.

BUSINESS IMPACT

You pay for seats nobody uses, staff sit on plans that do not include what they need, and when something goes wrong the licensing provider and the IT provider point at each other.

THE BASTION FIX

Licences supplied and managed by the same people who run your tenant, reviewed at every quarterly review so you are paying for the seats you actually use, and virtual desktops or hosted servers where a physical machine no longer makes sense.

WHAT WE SUPPLY AND MANAGE

We supply the full Microsoft range, from entry level mailboxes through to premium security and compliance plans, along with the add-ons most businesses end up needing. Where a physical machine no longer makes sense we move the workload to a virtual desktop or a hosted server.

SIGNS THIS APPLIES TO YOU

- Licences were bought ad hoc and never reviewed
- Staff sit on plans that do not include what they need
- Platform support sits with somebody who has never seen your setup
- Nobody reconciles seats when people leave

HOW YOU WILL KNOW IT IS WORKING

- Licence count reconciled against headcount each month
- Plan fit reviewed so nobody pays for capability they never use
- Tenant configuration documented and changes tracked
- One provider accountable for both the licence and the fix

NEXT STEP: COUNT YOUR PAID MICROSOFT LICENCES AGAINST YOUR CURRENT HEADCOUNT AND SEE WHETHER THE NUMBERS MATCH.

WEB, MAIL & DOMAINS

Hosted Infrastructure & Domains

Servers, mail, DNS and domain names held in one place, by the same provider who secures everything else.

THE PROBLEM

Domains sit in an account registered to a staff member who left, hosting is with a company nobody has spoken to in years, and DNS is managed by whoever built the website.

BUSINESS IMPACT

A domain quietly expires and takes email down with it, or nobody can make a DNS change when it matters because the login is gone. Both are avoidable and both are expensive.

THE BASTION FIX

Domains registered and renewed in an account your business owns, DNS managed by us with every record documented, and web and email hosting on infrastructure we control so a problem gets fixed rather than logged with somebody else's support queue.

WHAT WE PROVIDE

Virtual and hosted servers, web and email hosting, DNS, and domain registration across Australian and international extensions. All of it held in an account your business owns.

SIGNS THIS APPLIES TO YOU

- Your main domain is registered to a staff member who left
- Nobody can make a DNS change without hunting for a login
- Hosting is with a company you have not spoken to in years
- Renewal dates are not tracked anywhere

HOW YOU WILL KNOW IT IS WORKING

- Domains held in an account your business owns
- Every DNS record documented and changes logged
- Renewal dates tracked and actioned well before they lapse
- Server and hosting availability reported monthly

NEXT STEP: CHECK WHO THE REGISTRANT CONTACT IS ON YOUR MAIN DOMAIN, AND WHETHER THAT PERSON STILL WORKS FOR YOU.

VOICE & COMMUNICATIONS

Business Telephony

Hosted phone systems, numbers and call plans, run by the same team that runs your network. When the phones go down it is one call, not three vendors.

THE PROBLEM

The phone system, the internet service and the network come from three different companies. When a call drops, each one says the problem sits with the other two.

BUSINESS IMPACT

Customers cannot reach you, nobody owns the fault, and the business loses hours to something that should have taken one phone call to sort.

THE BASTION FIX

A hosted phone system sized to your headcount, running over an internet service we supply, on a network we manage. One provider accountable end to end, with call plans matched to how your team actually uses the phone rather than a bundle chosen for you.

WHAT WE PROVIDE

Hosted phone systems sized from a handful of concurrent calls up to a busy service desk, SIP trunking, inbound 1300 numbers, and call plans from pay as you go through to unlimited. We install analogue adapters where you have equipment worth keeping.

SIGNS THIS APPLIES TO YOU

- Phones, internet and network come from three different suppliers
- A dropped call turns into a three way blame conversation
- Changing a call flow means raising a ticket somewhere else
- You pay for lines nobody uses

HOW YOU WILL KNOW IT IS WORKING

- One provider accountable across phones, network and internet
- Call quality and outage events reported
- Call plan reviewed against what your team actually uses
- Call flow changes made without going through a third party

NEXT STEP: WORK OUT WHO YOU WOULD RING FIRST IF THE PHONES STOPPED, AND WHETHER THAT PERSON CAN ALSO SEE THE NETWORK.

03

Pillar Three

Provide Responsive Support

When something breaks you want a person who already knows your setup, not a queue. One owner per ticket, an Australian desk, and updates a non-technical manager can act on.

RESPONSIVE OWNERSHIP

Bastion Managed Services

THE PROBLEM

Being treated like a number in a queue, with tickets passed between technicians who each start the diagnosis from scratch.

BUSINESS IMPACT

Staff stop logging issues because logging them feels slower than working around them, and small faults quietly become expensive ones.

THE BASTION FIX

One owner per ticket from the moment it is logged until it is closed, an Australian service desk staffed by named people your team gets to know, and updates written in language a non-technical manager can act on.

☐ ONE OWNER PER TICKET

☐ PLAIN ENGLISH UPDATES

☐ AUSTRALIAN SERVICE DESK

☐ NAMED TECHNICAL LEAD

HOW SUPPORT IS PACKAGED

Support is packaged to suit the business, from a mail and security bundle with a support component through to an agreement with unlimited support and licensing included. We will tell you which one fits rather than putting you on the biggest.

SIGNS THIS APPLIES TO YOU

- ☐ Tickets get passed between technicians who each start over
- ☐ Staff work around problems instead of logging them
- ☐ You cannot tell what your provider actually did last month

HOW YOU WILL KNOW IT IS WORKING

- ☐ One named owner on every ticket until it closes
- ☐ Response and resolution measured against agreed targets
- ☐ The same named technical lead across the year

NEXT STEP: REVIEW HOW YOUR CURRENT PROVIDER HANDLES ESCALATIONS AND WHAT ACTUALLY HAPPENS TO A TICKET AFTER HOURS.

What happens when you log a ticket.

PRIORITY	DEFINITION	RESPONSE	RESOLUTION TARGET
P1	Business stopped. All users or a critical system offline, or a live security incident.	15 minutes	4 hours
P2	Major disruption. A team or a core function is unable to work, with no reasonable workaround.	1 hour	8 business hours
P3	Single user affected, or a fault with a workaround available.	4 business hours	2 business days
P4	Requests, changes, new starters, scheduled work.	1 business day	5 business days

COVERAGE

SERVICE DESK HOURS

Staffed 8am to 6pm, Monday to Friday. The service desk runs longer hours than our offices are open for walk-ins.

AFTER HOURS AND ESCALATION

After-hours phone support is available outside staffed hours, charged at our after-hours rate.

SECURITY OPERATIONS

Live 24/7 monitoring with automated daily checks and human verification weekly.

ON-SITE ATTENDANCE

On site across South East Queensland from Carindale, with a Luscombe office by appointment.

04

Pillar Four

Offer Clear Guidance

You should understand what you are paying for and what is protecting your data. Most providers profit from confusion. We would rather you knew exactly where you stand.

REPORTING & REVIEW

You always know where you stand

THE PROBLEM

IT reporting is either non-existent or it is a wall of green ticks that tells a business owner nothing they can act on. Nobody explains what was spent, what was at risk, or what is coming next.

BUSINESS IMPACT

Budget decisions get made blind, renewals get signed without anyone checking whether the licences are still needed, and risk only becomes visible after it turns into an incident.

THE BASTION FIX

Monthly executive reporting written for a business owner rather than a technician, a quarterly on-site review that covers what is coming instead of what broke, licensing reviewed so you are not paying for seats nobody uses, and a straight answer when the honest answer is that you do not need what we sell.

☐ MONTHLY EXECUTIVE REPORTING

☐ PLAIN ENGLISH UPDATES

☐ QUARTERLY ON-SITE REVIEWS

☐ COST AND LICENCE CLARITY

SIGNS THIS APPLIES TO YOU

- ☐ Your reporting is a wall of green ticks
- ☐ You cannot tell what changed since last month
- ☐ Renewals get signed without anyone checking the need
- ☐ Risk only becomes visible after something has gone wrong

HOW YOU WILL KNOW IT IS WORKING

- ☐ One monthly report a non-technical manager can act on
- ☐ What changed, what was at risk, and what it cost
- ☐ A quarterly session about what is coming, not what broke
- ☐ Recommendations with a price, and room to say no

NEXT STEP: ASK FOR YOUR LAST THREE MONTHS OF IT REPORTING, AND SEE WHETHER YOU CAN TELL WHAT CHANGED.

05

Pillar Five

Teach Your Team

Two kinds of teaching. The team that spots a dodgy email is your strongest control, and the team that knows how to use what you already pay for is your cheapest productivity win. Both need training that respects their time.

CULTURAL UPLIFT

Security Awareness

THE PROBLEM

Teams often bypass security measures because they find them frustrating or complex.

BUSINESS IMPACT

The human element remains the largest risk surface for cyber incidents.

THE BASTION FIX

Bite-sized micro-training and simple plain English policy playbooks.

- ☐ STAFF MICRO-TRAINING
- ☐ HABIT COACHING

- ☐ SIMPLE PLAYBOOKS
- ☐ PHISHING SIMULATIONS

SIGNS THIS APPLIES TO YOU

- ☐ Staff bypass controls because they find them annoying
- ☐ Nobody is sure how to report a suspicious email
- ☐ Training happens once a year, if at all
- ☐ The same few people keep clicking the same things

HOW YOU WILL KNOW IT IS WORKING

- ☐ Completion tracked per person, not per company
- ☐ Phishing simulation results trended over time
- ☐ Reporting rate measured, not just click rate
- ☐ Playbooks your staff can actually find when they need them

NEXT STEP: ASK YOUR TEAM HOW THEY REPORT A SUSPICIOUS EMAIL, AND SEE HOW MANY GIVE THE SAME ANSWER.

CAPABILITY UPLIFT

Solutions Training

Training on the tools you already pay for, Copilot and the rest of the Microsoft stack included, so your team actually uses what is sitting in their licence.

THE PROBLEM

Businesses buy Copilot and the premium plans, then nobody is shown how to use them. The licence gets paid every month and the team carries on working the way they always did.

BUSINESS IMPACT

You pay for capability you never see, staff stay slow at tasks the tools could do in seconds, and the case for the next investment gets harder because the last one showed no return.

THE BASTION FIX

Practical sessions run on your own systems and your own work, not a generic course off a shelf. We show people what the tools can do for the jobs they actually spend their week on, cover where AI is worth trusting and where it is not, then check back later to see what stuck.

- ☐ COPILOT IN YOUR BUSINESS
- ☐ MICROSOFT 365 SKILLS

- ☐ PRACTICAL AI USE CASES
- ☐ SESSIONS ON YOUR OWN DATA

SIGNS THIS APPLIES TO YOU

- ☐ You pay for Copilot and almost nobody opens it
- ☐ Premium licences bought, the capability never seen
- ☐ Staff do by hand what the tools already do in seconds
- ☐ Nobody has shown the team what is actually possible

HOW YOU WILL KNOW IT IS WORKING

- ☐ Licence usage measured against what you are paying for
- ☐ Sessions run on your own work, with what stuck checked later
- ☐ The tasks people stopped doing by hand, named
- ☐ A straight view of where AI helps and where it does not

NEXT STEP: ASK HOW MANY OF YOUR STAFF HAVE OPENED COPILOT THIS MONTH, THEN COMPARE IT TO HOW MANY LICENCES YOU ARE PAYING FOR.

Technical controls by pillar.

PILLAR	SERVICE	CONTROLS IN PLACE
01 Manage Risk	Bastion Cybersecurity	Continuous vulnerability scans, identity hardening, endpoint protection (EDR), patch velocity targets
01 Manage Risk	Managed Security Tiers	Four tiers priced per device and stacked, from email and Microsoft 365 protection through to application control and full disaster recovery
01 Manage Risk	Microsoft 365 & Identity	Full MFA coverage, conditional access policies, mailbox rule monitoring, licence optimisation
01 Manage Risk	Network & Connectivity	Network segmentation, monitored firewalls, DNS and web filtering, managed wireless, business internet, failover, cabling and equipment supply
01 Manage Risk	Physical Security	Segmented camera networks, door and access control, managed firmware and credentials, retention set to policy
02 Ensure Continuity	Backup & Recovery	Desktop, server and Microsoft 365 coverage, scheduled restore testing, documented recovery process, annual retention review
02 Ensure Continuity	Cloud Solutions	Microsoft 365 licensing and tenant management, virtual desktops and hosted servers, migration
02 Ensure Continuity	Hosted Infrastructure	Virtual private servers, hosted servers, web and email hosting, DNS hosting, domain registration and renewal
02 Ensure Continuity	Business Telephony	Hosted phone systems, SIP trunks, call plans, inbound numbers, analogue adapter installation
02 Ensure Continuity	Hardware & Procurement	Standard device builds, identity and device enrolment, asset and warranty register, consumables supply
03 Responsive Support	Bastion Managed Services	One owner per ticket, Australian service desk, plain English updates, named technical lead
04 Clear Guidance	Reporting & Review	Monthly executive reporting, quarterly on-site reviews, plain English updates, cost and licence clarity
05 Teach Your Team	Security Awareness	Staff micro-training, simple playbooks, habit coaching, phishing simulations
05 Teach Your Team	Solutions Training	Copilot and Microsoft 365 skills, practical AI use cases, sessions run on your own data

VERIFICATION

Every control above is checked automatically each day and verified by a person each week. Findings that need your decision go into the monthly report rather than sitting in a queue nobody reads.

How we take you on.

We don't rip and replace on day one. We find out what you have, fix what is actually dangerous, then work through the rest in a sensible order so your team keeps working the whole way through. Most onboardings run start to finish inside two weeks.

01

Days 1 to 3

Discovery

We map what you actually have. Every device, every user, every licence, every domain, every phone line and every piece of network hardware. We check backups, MFA coverage, admin accounts and what is exposed to the internet.

02

Days 4 to 5

Findings and priorities

You get the findings in plain English, sorted by risk, with the cost of fixing each one. Nothing is bundled to hide a price. If something is already set up well, we tell you and we leave it alone.

03

Days 6 to 8

Stabilise

We close the dangerous gaps first. MFA across every account, backups verified with a real test restore, monitoring and endpoint protection deployed, admin access cut back to who genuinely needs it.

04

Days 9 to 10

Transition and documentation

Licences, domains, hosting and phone services move across at a pace that does not interrupt anyone. Your environment gets documented properly, so knowledge sits with your business rather than in one technician's head.

05

Ongoing

Steady state

All five pillars running together. Automated daily checks, human verification weekly, monthly executive reporting you can actually read, and a quarterly on-site review where we sit down and talk about what is coming rather than what broke.

NEXT STEP

If we can help, we will. If not, we'll tell you.

The honest way to start is a conversation, not a quote. Give us a ring and we will have a look at where you stand across the five pillars. If your current setup is in good shape, you will hear that from us.

PHONE

1300 900 222

EMAIL

support@bastionit.com.au

WEB

bastionit.com.au

SERVICE AREA

South East Queensland

COMPANY DETAILS

Registered entity: Bastion Cybersecurity & Managed Services Pty Ltd

Trading as: Bastion IT

ABN: 71 696 276 187, GST registered

Head office: 23 Bridgnorth St, Carindale QLD 4152

By appointment: Level 2, 4 Aliciajay Cct, Luscombe QLD 4207

Insurances: \$20 million professional indemnity, \$10 million public liability

Accreditations: SMB1001 Gold, Microsoft Partner (Bronze), 3CX Silver Partner

